NOKIA

Nokia Intellisync Mobile Suite Administrator's Guide

Version 9.0

Published May 2008

050208

Nokia Contact Information

Corporate Headquarters

Web Site	http://www.nokia.com
Telephone	1-888-477-4566 *or* 1-650-625-2000
Fax	1-650-691-2170
Mail Address	Nokia Inc. 313 Fairchild Drive Mountain View, California 94043-2215 USA

Regional Contact Information

Americas	Nokia Inc. 313 Fairchild Drive Mountain View, CA 94043-2215 USA	Tel: 1-877-997-9199 Outside USA and Canada: +1 512-437-7089 email: info.ipnetworking_americas@nokia.com
Europe, Middle East, and Africa	Nokia House, Summit Avenue Southwood, Farnborough Hampshire GU14 ONG UK	Tel: UK: +44 161 601 8908 Tel: France: +33 170 708 166 email: info.ipnetworking_emea@nokia.com
Asia-Pacific	438B Alexandra Road #07-00 Alexandra Technopark Singapore 119968	Tel: +65 6588 3364 email: info.ipnetworking_apac@nokia.com

Nokia Customer Support

Web Site:	https://support.nokia.com/		
Americas		**Europe**	
Voice:	1-888-361-5030 or 1-613-271-6721	**Voice:**	+44 (0) 125-286-8900
Fax:	1-613-271-8782	**Fax:**	+44 (0) 125-286-5666
Asia-Pacific			
Voice:	+65-67232999		
Fax:	+65-67232897		

050602

Contents

About this Guide

In This Guide

This guide is organized into the following chapters and appendixes:

- Chapter 1, “Introducing Nokia Intellisync Mobile Suite,” introduces you to Nokia Intellisync Mobile Suite and provides information for using Nokia Intellisync Mobile Suite effectively.
- Chapter 2, “Using the Admin Console,” covers information for setting up and using the Nokia Intellisync Mobile Suite control.
- Chapter 3, “Using Management Tools,” covers the Management control and its functions.
- Chapter 4, “Profile Settings,” contains the information you need to effectively use Profile Settings in the Nokia Intellisync Mobile Suite control.
- Chapter 5, “Security,” provides an overview of Intellisync’s security capabilities and how you can use these strategies with your corporate security plan.
- Chapter 6, “Network Configuration,” contains information to configure your network for secure synchronization traffic.
- Chapter 7, “Authenticating Users,” provides an overview of setting up authentication so user can connect to the Nokia Intellisync Mobile Suite server.
- Chapter 8, “Granting Access to the Mail Server,” provides steps to grant user access to the mail server.
- Chapter 9, “Maintaining Nokia Intellisync Mobile Suite,” covers information on backing up your system.
- Appendix A, “Client APIs,” includes a comprehensive set of application program interfaces (APIs) for the Nokia Intellisync Mobile Suite Client.

Additional information provided in this section is as follows:

- Conventions This Guide Uses
- Terminology
- Related Documentation

Conventions This Guide Uses

The following sections describe the conventions this guide uses, including notices, text conventions, and command-line conventions.

Notices

Warning
Warnings advise the user that bodily injury might occur because of a physical hazard.

Caution
Cautions indicate potential equipment damage, equipment malfunction, loss of performance, loss of data, or interruption of service.

Note
Notes provide information of special interest or recommendations.

Command-Line Conventions

You might encounter one or more of the following elements on a command-line path.

Table 1 Command-Line Conventions

Convention	Description
command	This required element is usually the product name or other short word that invokes the product or calls the compiler or preprocessor script for a compiled Nokia product. It might appear alone or precede one or more options. You must spell a command exactly as shown and use lowercase letters.
Italics	Indicates a variable in a command that you must supply. For example: **`delete interface if_name`** Supply an interface name in place of the variable. For example: **`delete interface nic1`**
angle brackets < >	Indicates arguments for which you must supply a value: **`retry-limit <1–100>`** Supply a value. For example: **`retry-limit 60`**

Table 1 Command-Line Conventions (*continued*)

Convention	Description
Square brackets [ ]	Indicates optional arguments. **`delete [slot slot_num]`** For example: **`delete slot 3`**
Vertical bars, also called a *pipe* (|)	Separates alternative, mutually exclusive elements. **`framing <sonet | sdh>`** To complete the command, supply the value. For example: **`framing sonet`** or **`framing sdh`**
-flag	A flag is usually an abbreviation for a function, menu, or option name, or for a compiler or preprocessor argument. You must enter a flag exactly as shown, including the preceding hyphen.
.ext	A filename extension, such as .ext, might follow a variable that represents a filename. Type this extension exactly as shown, immediately after the name of the file. The extension might be optional in certain products.
(. , ; + * - /)	Punctuation and mathematical notations are literal symbols that you must enter exactly as shown.
' '	Single quotation marks are literal symbols that you must enter as shown.

Text Conventions

Table 2 describes the text conventions in this guide.

Table 2 Text Conventions

Convention	Description
`monospace font`	Indicates command syntax, or represents computer or screen output, for example: `Log error 12453`
Key names	Keys that you press simultaneously are linked by a plus sign (+): Press Ctrl + Alt + Del.
Menu commands	Menu commands are separated by a greater than sign (>): Choose File > Open.
The words enter and type	Enter indicates you type something and then press the Return or Enter key. Do not press the Return or Enter key when an instruction says *type*.
Italics	• Emphasizes a point or denotes new terms at the place where they are defined in the text. • Indicates an external book title reference. • Indicates a variable in a command: `delete interface` *`if_name`*

Terminology

The following abbreviations are used throughout the Nokia Intellisync Mobile Suite documentation library.

Acronym	Definition
ADSI	**A**ctive **D**irectory **S**ervices **I**nterface
API	**A**pplication **P**rogram **I**nterface
DMZ	**D**e**m**ilitarized **Z**one
HTTP	**H**yper**t**ext **T**ransfer **P**rotocol
HTTPS	A more secure version of HTTP
LAN	**L**ocal **a**rea **n**etwork
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
MAPI	**M**essaging **A**pplication **P**rogramming **I**nterface

MMC	**M**icrosoft **M**anagement **C**onsole
PIM	**P**ersonal **I**nformation **M**anager
RAS	**R**emote **A**ccess **S**erver
RSA	**R**ivest-**S**hamir-**A**dleman encryption
SMS	**S**ystems **M**anagement **S**erver
SSL	**S**ecure **S**ockets **L**ayer
TCP	**T**ransmission **C**ontrol **P**rotocol
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol

Related Documentation

Nokia offers a common framework for the Intellisync Mobile Suite products. For this reason, there are electronic manuals and online help systems that cover the entire suite, plus additional resources for specific products.

For instructions to access documentation, see the following topics:

- "Accessing Server Documentation"
- "Accessing Client Documentation"

Accessing Server Documentation

In addition to this guide, there are several other documents in electronic format that are available.

Server Guides

The following server guides are available for Wireless Email. These documents are available on the Nokia Support Web site (https:// support.nokia.com) in Adobe Portable Document Format (PDF).

Nokia Intellisync Mobile Suite Installation Guide (InstallGdeEN.pdf) Includes the installation requirements and other information you need to install Nokia Intellisync Mobile Suite software for servers and clients. This guide applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Mobile Suite Administrator's Guide (AdminGdeEN.pdf) Includes an introduction to the suite and general information about using the suite successfully (this guide). This guide applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Device Management and File Sync Administrator's Guide (DeviceMgmtFileSyncGdeEN.pdf) Written as a companion book to the administrator's guide. Covers available functions and features with Device Management and File Sync.

Nokia Intellisync Corporate Email Connector Configuration Guide (CECConfigGdeEN.pdf) Covers system requirements and installation procedures for Corporate Email Connector installations using Lotus Domino and/or Microsoft Exchange.

Nokia Intellisync Secure Gateway Administrator's Guide (SecureGatewayGdeEN.pdf) Written as a companion book to the Nokia Intellisync Mobile Administrator's Guide. Covers administrative functions for managing the Secure Gateway.

Nokia Intellisync Mobile Suite Release Notes (ReleaseNotesEN.pdf) Includes important information you should know before you install and use Nokia Intellisync Mobile Suite. Also includes important late-breaking information that may not be included in other documentation. This document applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Server Online Help

The following online help systems are embedded in the server applications.

Nokia Intellisync Mobile Suite WebAdmin Console Help Includes information related to the managing the server using a Web browser.

Nokia Intellisync Mobile Suite (MMC) Admin Console Help – Management (ManagementHelpEN.chm) Includes information related to the Management control on the MMC console tree, such as Users, Groups, Reports, and Logs. This help system applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Mobile Suite (MMC) Admin Console Help – Profile Settings (ProfileHelpEN.chm) Includes information to help you use profile settings effectively. This help system applies to the entire suite and is shared with other Nokia Intellisync Mobile Suite products.

Nokia Intellisync Mobile Suite Device Management/File Sync Help (iSMiFDEN.chm) Includes information specific to Device Management and File Sync.

Accessing Client Documentation

The following electronic client documents are available on the Nokia Support Web site (https://support.nokia.com) in Adobe Portable Document Format (PDF).

Client Installation and Setup Guides

Each guide includes information for installing software on devices using a specific platform, setting synchronization settings, and synchronizing for the first time.

Table 3 Client Guides

Name	File Name
Nokia Intellisync Mobile Suite Client Guide - Palm OS Platform	PalmUsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - Pocket PC Platform	PPCUsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - Smartphone Platform	SmartphoneUsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - S60 3rd Edition Platform	Symbian60_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - S80 Platform	Symbian80_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - UIQ Platform	SymbianUIQ_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - UIQ 3rd Edition Platform	SymbianUIQ3_UsersGuideEN.pdf
Nokia Intellisync Mobile Suite Client Guide - J2ME Platform	J2ME_UsersGuideEN.pdf

Note
The client guides are *not* installed as part of the client installation. You decide whether to provide this documentation to your users.

Client Online Help

The following online help systems are embedded in the Wireless Email client application.

Nokia Intellisync Mobile Suite PC Client Help Includes information about using the Nokia Intellisync Mobile Suite Client on a PC.

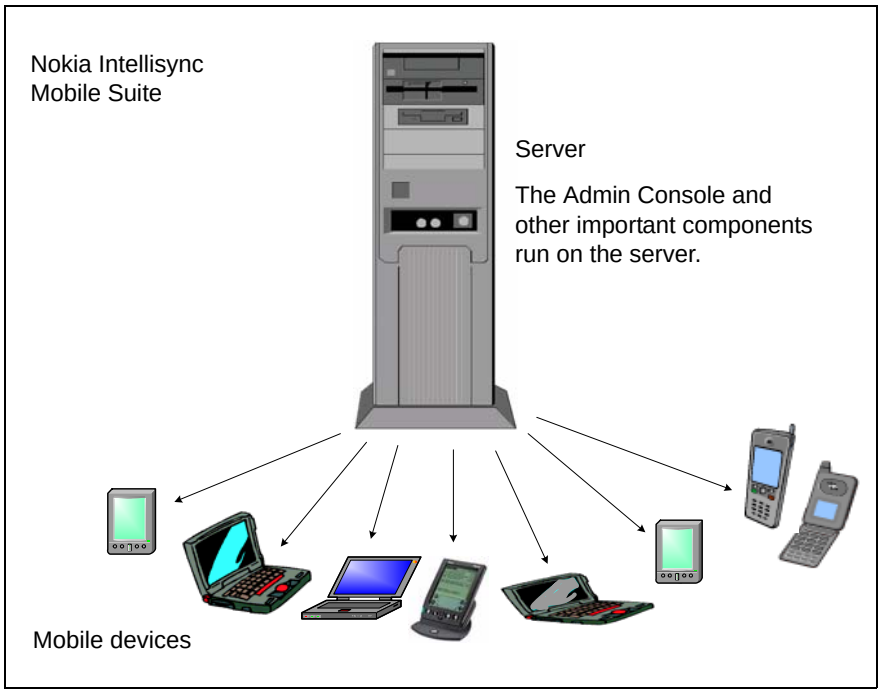
Nokia Intellisync Mobile Suite Web PIM Help Includes information about using the Nokia Intellisync Mobile Suite Client on a PC.

1 Introducing Nokia Intellisync Mobile Suite

Nokia Intellisync Mobile Suite is a collection of products designed to help you support your mobile workforce through a single-source solution to meet your mobile computing needs.

Nokia Intellisync Mobile Suite consists of both server and client components that facilitate interaction with the server. The server is the data synchronization host to which mobile devices connect. The server Admin Console controls functions such as security, user authentication, communication, logging, and reporting, among others.

Figure 1 Nokia Intellisync Mobile Suite Includes Software for Server and Clients



Different versions of the Nokia Intellisync Mobile Suite client software are available for the following device platforms:

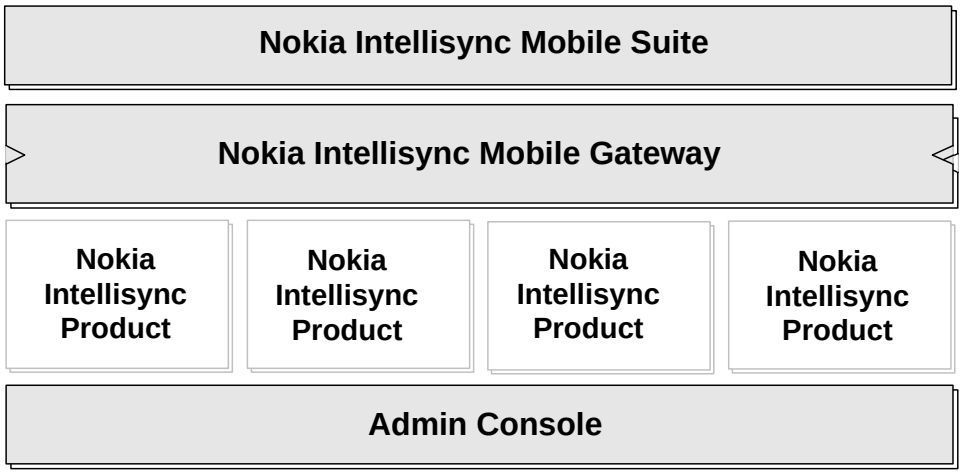
- Windows Mobile Pocket PC and Smartphone
- Symbian S60 3rd Edition
- Symbian UIQ 2nd Edition
- Symbian S80
- Palm
- J2ME

Nokia Intellisync Mobile Suite Components

Nokia Intellisync Mobile Suite is built around a set of core technologies that provide a common structure and for all components presented through a single user interface. This framework extends your enterprise system to include a wide variety of devices and networks.

Nokia Intellisync Mobile Suite 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. All Nokia Intellisync Mobile Suite products include this basic infrastructure.

Figure 2 Nokia Intellisync Mobile Suite Basic Infrastructure



Nokia Intellisync Mobile Suite Client

The Nokia Intellisync Mobile Suite client application provides users with easy access to information available through your server. The client application runs on client computers and mobile devices. This is the only application an end user needs to stay connected while away from the office.

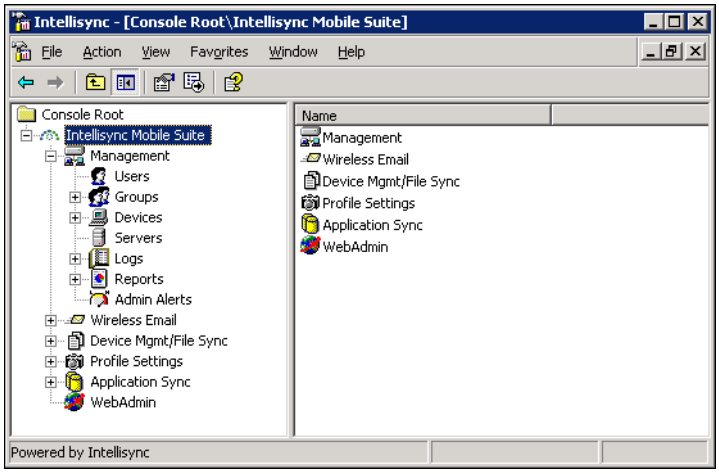
The client has an easy-to-use user interface and serves as the user's launch pad for delivery of all mobile information. After a synchronization session, the user sees a summary of the new information. The user can also view summary information for previous sessions.

Nokia Intellisync Mobile Gateway

The Nokia Intellisync Mobile Gateway handles communication, connection, security and encryption, and user authentication. The Mobile Gateway is the connection between the server and the outside world. Mobile Gateway is installed as part of the server installation. The client software contains the components required to connect to the server through the Mobile Gateway.

Nokia Intellisync Mobile Suite Control

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



In addition to the Nokia Intellisync Mobile Suite control, you can use the Web-based Admin Console, WebAdmin, from a browser to manage users, groups, and devices. For more information on the WebAdmin feature, refer to "WebAdmin" on page 47.

From the Nokia 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 Nokia Intellisync Mobile Suite product
- Managing profile settings
- Configuring connectivity settings

Because the Nokia 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. The custom console becomes the central place where you manage users for all products. Microsoft SQL Server is an example of MMC-compatible products that you can add and manage from the Nokia Intellisync Mobile Suite control.

The Nokia Intellisync Mobile Suite control is installed as part of the server installation.

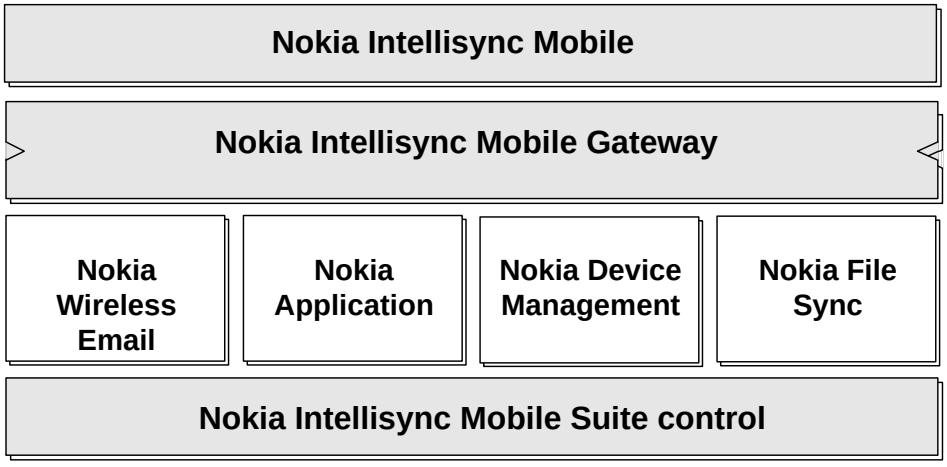
Nokia Intellisync Mobile Suite Products

The Nokia Intellisync Mobile Suite infrastructure contains the basic elements in your mobile solution. In addition to this framework, four separate products are available for you to purchase to support your mobile workforce. Nokia offers the following products as part of Nokia Intellisync Mobile Suite:

- Wireless Email
- Application Sync
- File Sync
- Device Management

These products snap into the Nokia Intellisync Mobile Suite framework. You can use the products together or separately.

Figure 3 Nokia Intellisync Mobile Suite with Products Installed

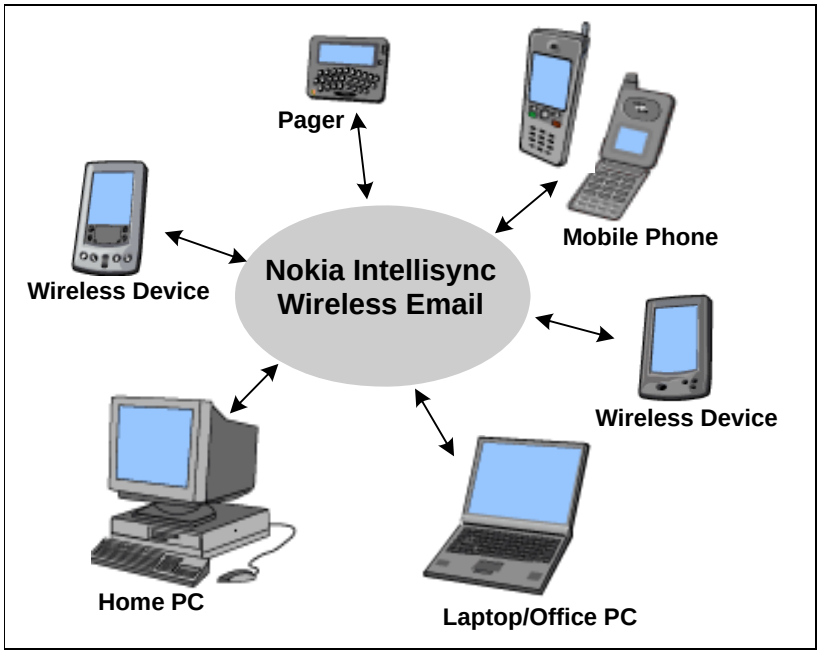


Wireless Email

Wireless Email offers centralized email and personal information manager (PIM) synchronization capabilities for your users. Wireless Email allows users to synchronize email, contacts, memos, calendar, and to-do items among all their mobile devices, eliminating duplicate data entry.

This same data is accessible from any Internet-capable mobile phone and the Web browser on any computer connected to the Internet

Figure 4 Universal Synchronization Using Wireless Email



Wireless Email also provides useful information based on your users' travel and appointment plans, such as weather, travel itinerary, maps, directions, and other content. Users can receive custom alerts for itinerary summaries and meeting reminders on a wireless phone or pager.

Application Sync

Application Sync synchronizes and distributes relational data among client computers that are intermittently connected to a server. Application Sync supports data synchronization for multiple combinations of databases.

Application Sync software is integrated with your company's applications, enabling synchronization without changes to your application. Application Sync captures changes from every client user, stores the changes and forwards them to the users you specify in your data sharing rules. Because Application Sync sends only the changed data to specific users, you can reduce communication costs and security risks.

File Sync

Using File Sync, you can send files or content to mobile users and also collect files or content from users.

File Sync is based on a publish-and-subscribe model. You can make files available to your users by creating packages called *publications*. These publications can remove directories, execute programs or scripts, copy files, delete files, move files, or rename files. You can also control who receives specific files by subscribing users to the files. File Sync can deliver documents of any file type, including Microsoft Word documents, Excel spreadsheets, and HTML pages.

From the Nokia Intellisync Mobile Suite control, you can create and associate packages with specific users, thereby creating a subscription. As part of the publication package, you can assign actions or create instruction scripts to run functions such as editing registry entries or launching programs.

After you associate a user with a publication, the user automatically receives updates to any file in that publication.

Device Management

Device Management allows the system administrator to collect and manage asset and inventory information for client devices. You can schedule the collection of this asset information, as well as choose specific assets to include in those collections.

Device Management also delivers software packages and updates to your client computers. Using the Nokia Intellisync Mobile Suite control, you can set up publications for software installation and maintenance. These publications can accomplish a variety of tasks:

- Remove directories
- Execute programs or scripts
- Copy, delete, move, or rename files
- Return client system information
- Add or delete registry keys

You can require the client computer to receive these publications or send the publications upon request.

From the Nokia Intellisync Mobile Suite control, you can track the versions of publications to ensure users receive the most recent software packages.

Microsoft Management Console

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

Server Database

Nokia Intellisync Mobile Suite requires a database to operate. The database stores your users, groups, publications, logs, and other important data. Nokia 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.

Note
For a complete list of installation requirements, see the *Nokia Intellisync Mobile Suite Installation Guide*.

2 Using the Admin Console

The Nokia Intellisync Mobile Suite control, also known as the Admin Console, is the center for all Nokia Intellisync Mobile Suite products on the server. You can complete many administrative tasks, including:

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

Before using the Nokia Intellisync Mobile Suite control, you must configure database and authentication settings.

Getting Started

The Admin Console is available on the server computer.

To start the Admin Console

1. Choose Start > Programs > Nokia Intellisync Mobile Suite > Admin Console.

   The Nokia Intellisync Mobile Suite control appears.

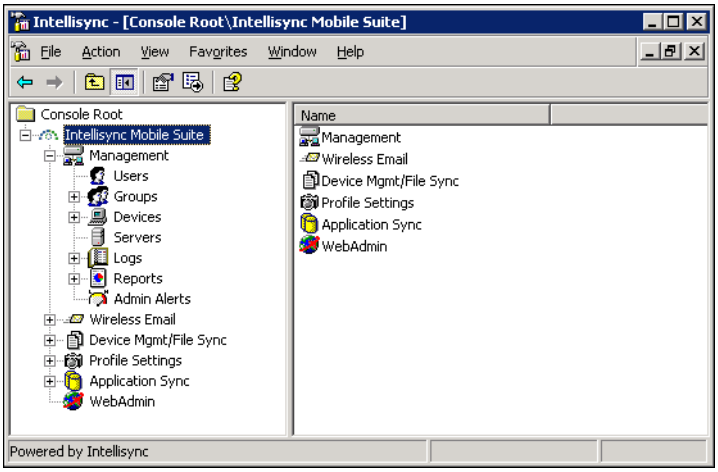
2. From the console tree, select Nokia Intellisync Mobile Suite to expand it.

   The Management and Profile Settings controls appear, in addition to controls for other Nokia Intellisync Mobile Suite products installed on your server. The Management and Profile Settings controls are common to all applications.

3. Select a control to view additional information.

Operating Conventions

Because the Nokia 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, as the following example shows.



Using the Action Menu

Within the Nokia Intellisync Mobile Suite control, there is a custom Action menu available for most items in the console tree.

1. From the console tree, select any control item.
2. From the menu bar, choose Action to see the functions available for that particular control.

The Action menu offers functions appropriate within the context of each control. For that reason, the menu items are different, depending on your location within the console tree. You can access most of the same menu items available from the Action menu by right-clicking the item in the tree.

Adding Other MMC-compatible Products

If you are using other MMC-compatible products to manage Nokia Intellisync Mobile Suite, 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, creating one central place to manage functions related to Nokia Intellisync Mobile Suite operations.

Actions and Properties

The Nokia 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 Nokia Intellisync Mobile Suite.
2. From the menu bar, choose Action. The Action menu appears.

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

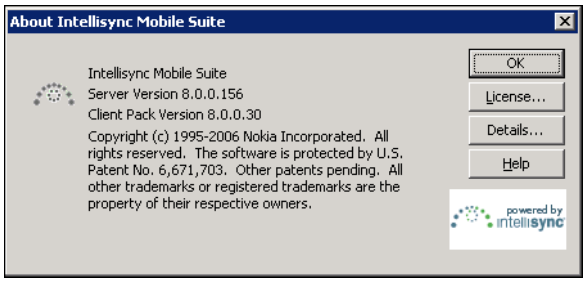
- About Nokia Intellisync Mobile Suite control
- Properties

These menu items are covered in the following pages.

Viewing the About Window

To view the About window

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. From the Action menu, choose About Nokia Intellisync Mobile Suite. The About Nokia Intellisync Mobile Suite dialog box appears.



The About window shows copyright information and version numbers for the Nokia Intellisync software and components.

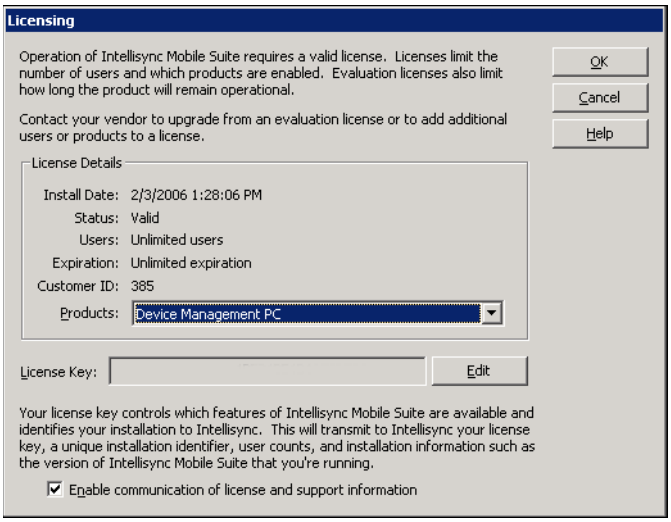
Viewing Your License Information

To view your current license information

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. From the Action menu, choose About Nokia Intellisync Mobile Suite.

   The About Nokia Intellisync Mobile Suite dialog box appears.
3. Choose License.

The Licensing dialog box appears.



Your license is based on the products and number of licenses you purchase. Evaluation licenses expire; however, production licenses do not. To upgrade your license or increase your number of licensed users, contact your sales representative.

Nokia Intellisync Mobile Suite Properties

To view the Nokia Intellisync Mobile Suite properties

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. From the Action menu, choose Properties. The Nokia Intellisync Mobile Suite Properties dialog box appears.

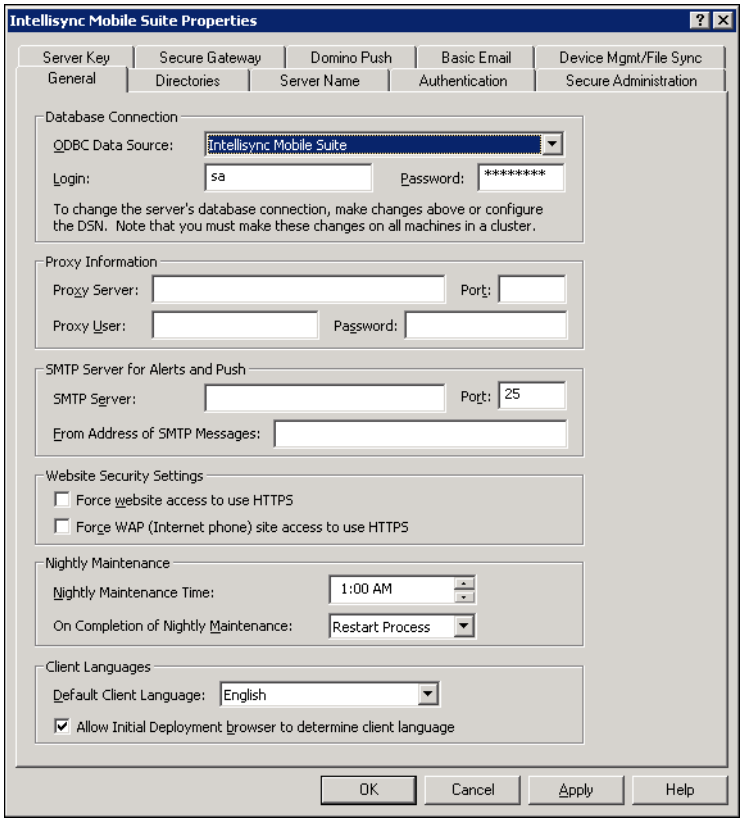
Use the sections that follow for descriptions of each panel. Your Nokia Intellisync Mobile Suite product installations determine which tabs and options appear.

General Tab

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

To view the Properties General tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties. The Nokia Intellisync Mobile Suite Properties dialog box appears. The General tab is the initial view.



Database Connection

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

Field	Description
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 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 you change the login and password in the database, you must also modify the Database Connection properties in the Nokia Intellisync Mobile Suite control.

Proxy Information

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

Field	Description
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 the Nokia Intellisync Mobile Suite server.

Web Site Security Settings

For additional security, you can force Web access, WAP access, or both to use HTTPS, 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.

Field	Description
Force Web Site 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.

Field	Description
Nightly Maintenance Time	You can configure the Nokia 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. Nokia strongly recommends that you select the default setting, Restart Process.

Client Languages

Use this section to set the default client language.

Field	Description
Default Client Language	Select a language for 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.

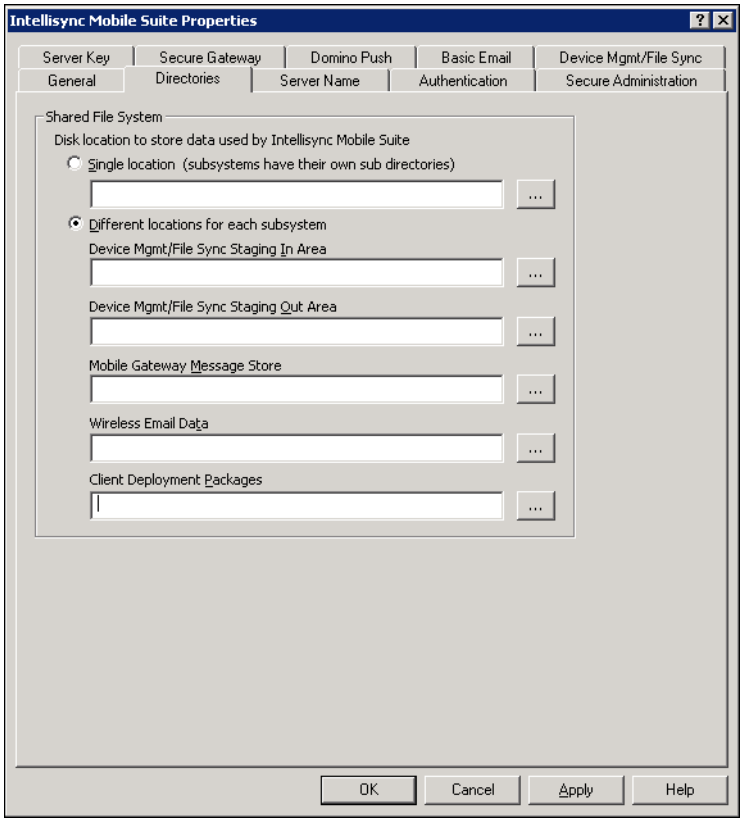
Directories Tab

Use the Directories tab to specify where you want to store Nokia Intellisync Mobile Suite data. You can use a single directory where subsystems reside in subdirectories, or you can specify separate directory locations for each subsystem.

To view the Properties Directories tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties. The Nokia Intellisync Mobile Suite Properties dialog box appears.
3. Choose the Directories tab.

The Directories panel appears.



4. Use the following information to set locations for storing Nokia Intellisync Mobile Suite data.

Field	Description
Single Location (Subsystems Have Their Own Subdirectories)	Type the path for storing Nokia Intellisync Mobile Suite data. Any subsystems reside in separate subdirectories.
Different Locations For Each Subsystem	Type a unique path for each subsystem.

Server Name Tab

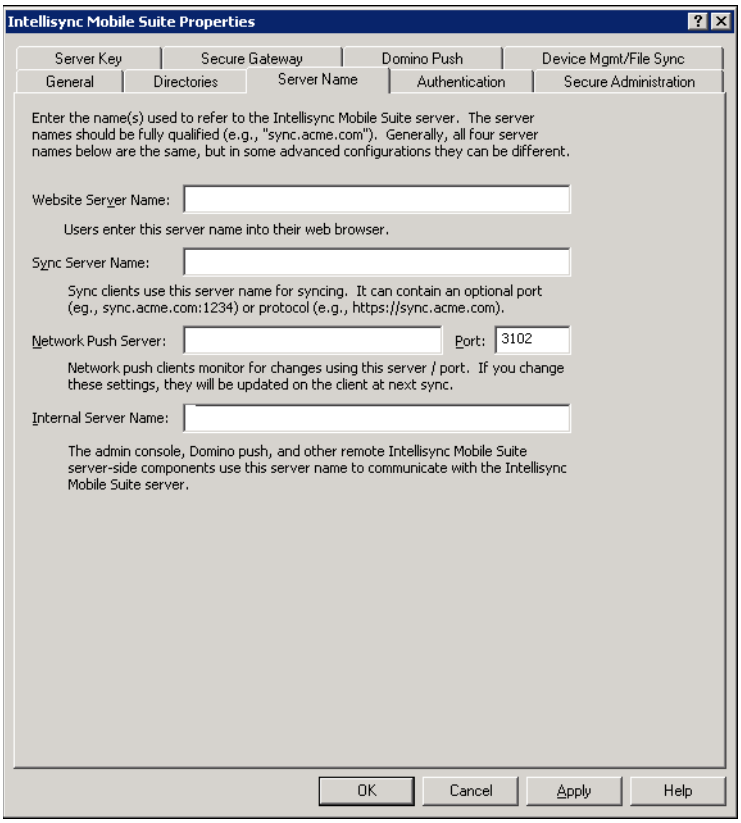
Use the Server Name tab to specify the server names that are part of your Nokia Intellisync Mobile Suite system. Use fully qualified server names. Usually, all server names are the same. In some advanced configurations, the server names may be different from each other. The Web site and sync server names may 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.

To view the Properties Server Name tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   The Nokia Intellisync Mobile Suite Properties dialog box appears.
3. Choose the Server Name tab.

   The Server Name panel appears.



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

Field	Description
Web Site 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.

Field	Description
Internal Server Name	The server name that the Nokia Intellisync Mobile Suite control (local or remote), Domino push, and other internal components use to communicate with the Nokia Intellisync server.

Authentication Tab

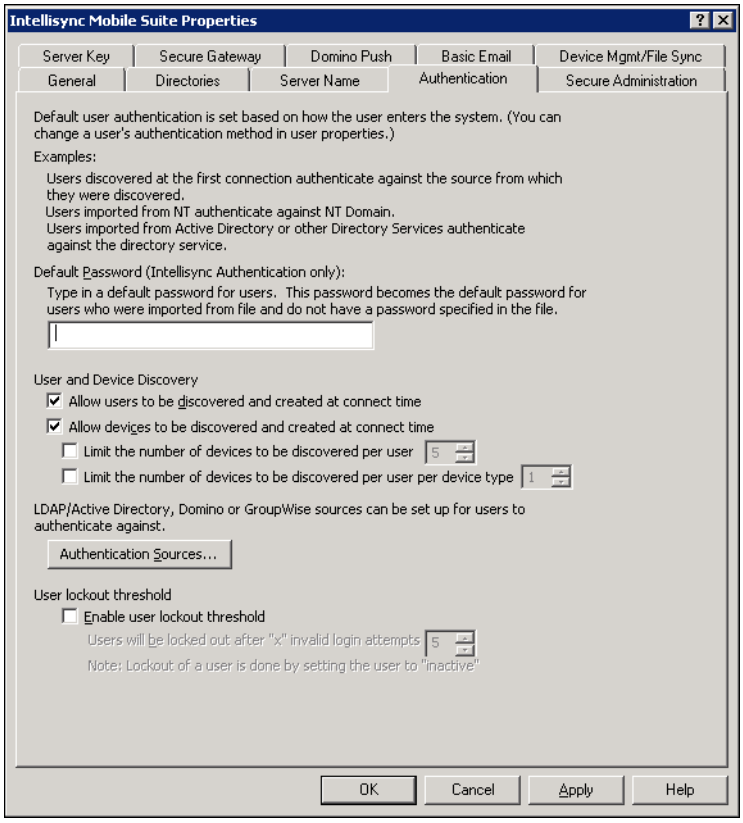
By default, Nokia Intellisync Mobile Suite authenticates a user by how the user enters the system. For example, if you import a user from a Windows NT domain, then Nokia Intellisync Mobile Suite uses NT Domain authentication by default. You can change a user's authentication method in Users Properties. For more information, see Chapter 7, "Authenticating Users."

To view the Properties Authentication tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   The Nokia Intellisync Mobile Suite Properties dialog box appears.
3. Choose the Authentication tab.

   The Authentication tab appears.



4. Use the following information to set options related to authentication.

Field	Description
Default Password (Nokia Intellisync Authentication Only)	Use this field to supply a password for imported who do not have a password specified in the file. (This field applies for Nokia 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 only authenticate devices that are existing in the system.
Authentication Sources	Choose Authentication Sources if you want to set up additional authentication sources, such as Active Directory/LDAP, Domino, or GroupWise. Windows NT and Nokia Intellisync authentication are available as soon as the Nokia Intellisync Mobile Suite server software installation completes.

Note
For additional information and guidelines for setting up authentication, see Chapter 7, "Authenticating Users."

Secure Administration Tab

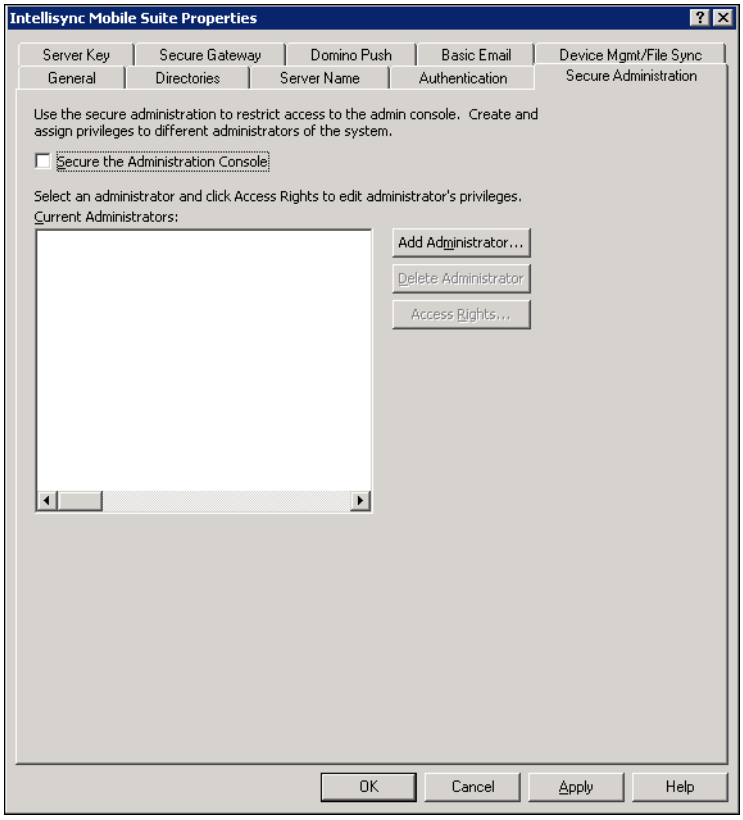
Use the Secure Administration tab to set permissions and restrict access to the Nokia Intellisync Mobile Suite control.

To view the Properties Secure Administration tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   The Nokia Intellisync Mobile Suite Properties dialog box appears.
3. Choose the Secure Administration tab.

The Secure Administration tab appears.



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

Field	Description
Secure The Administration Console	Select this option to restrict access to the Nokia Intellisync Mobile Suite control. Only users you specify as administrators can access the Nokia Intellisync Mobile Suite control when you enable this option.
Add Administrator	Choose Add Administrator to create control administrators and grant permission to additional users.

Server Key Tab

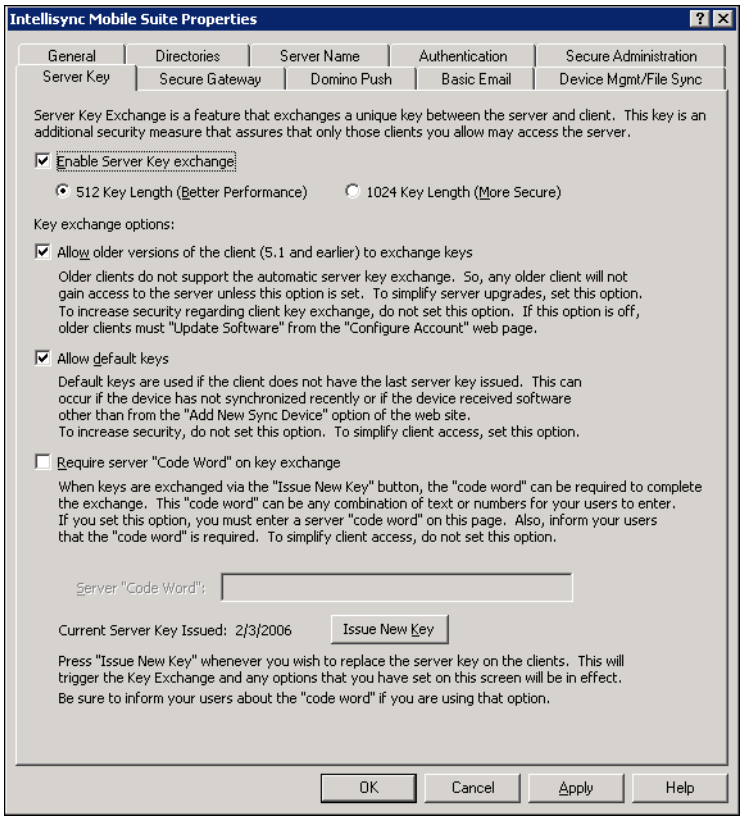
Use the Server Key tab to enable Server Key Exchange, a security feature that exchanges a unique key between the server and the clients.

To view the Properties Server Key tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

The Nokia Intellisync Mobile Suite Properties dialog box appears.

3. Choose the Server Key tab.



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

Field	Description
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.
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 clear this option, only clients running current software can participate in key exchange. That is, devices running older versions of client software cannot connect.

Field	Description
Allow Default Keys	Although this setting slightly decreases security, it simplifies access for clients. With this option set, Nokia 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	Choose Issue New Key when you want 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

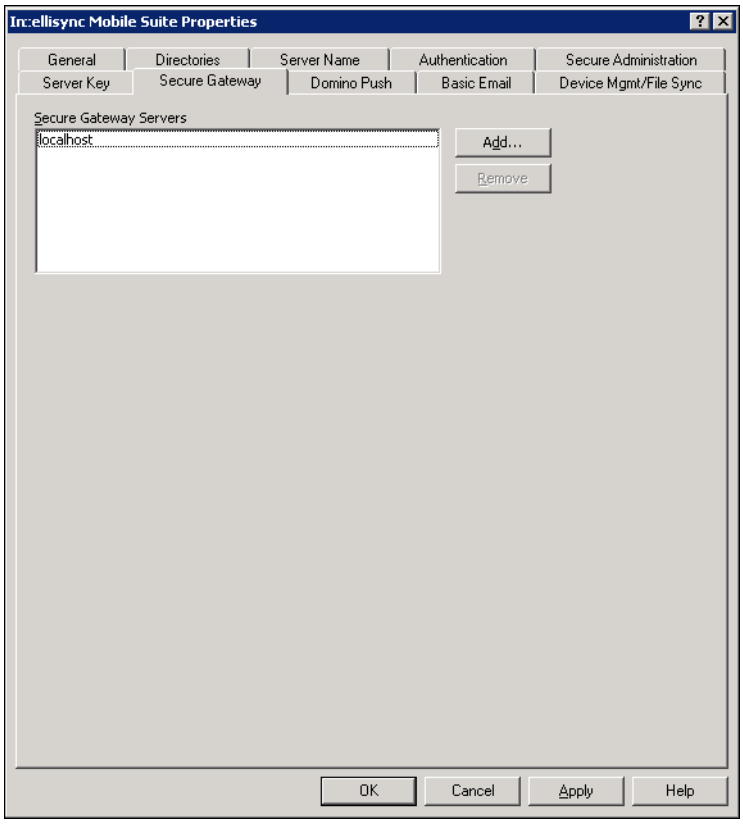
Use the Secure Gateway tab to add or remove Secure Gateway servers to your system. You can also change the port number that the Secure Gateway servers use. In most cases, the default port number setting is sufficient.

To view the Properties Secure Gateway tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   The Nokia Intellisync Mobile Suite Properties dialog box appears.

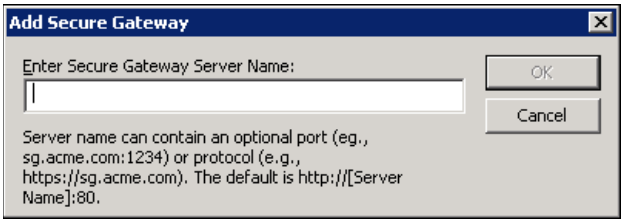
3. Choose the Secure Gateway tab.



Adding a Secure Gateway server

1. From the Secure Gateway panel, choose New.

   The Add Secure Gateway dialog box appears.



2. Type the name of the Secure Gateway server you want to add, and then choose OK. The server appears in the list on the Secure Gateway panel.
3. Select the server in the list, and then add the correct port number.
4. Choose OK.

Domino Push Tab

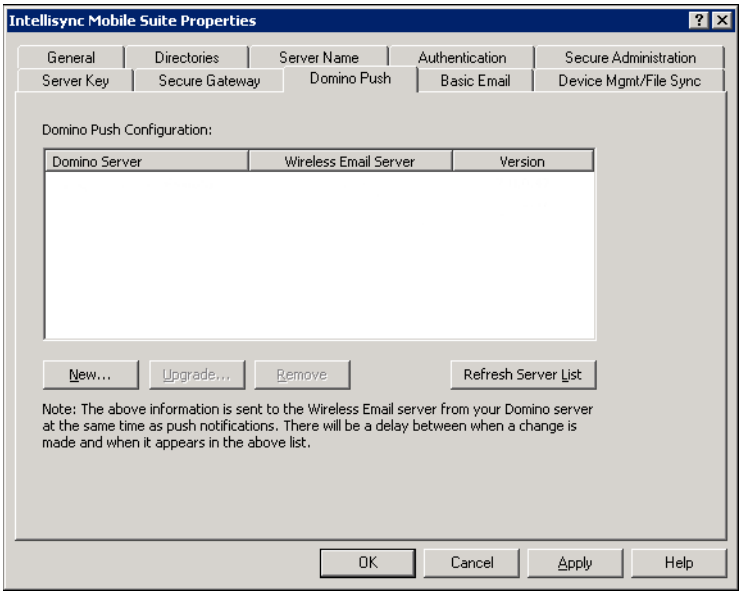
The Domino Push tab lists Domino servers set up for Push and the corresponding Wireless Email Server you want to notify when changes take place. For a server to appear on the list, it must successfully send a Push notification to the Wireless Email server. After adding a Push server, there may be a delay before the server appears on the list.

To view the Properties Domino Push tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   Nokia Intellisync Mobile Suite Properties dialog box appears.
3. Choose the Domino Push tab.

   The Domino Push panel appears. (The Domino Push tab is available only if you have Nokia Intellisync Wireless Email installed on your server.)



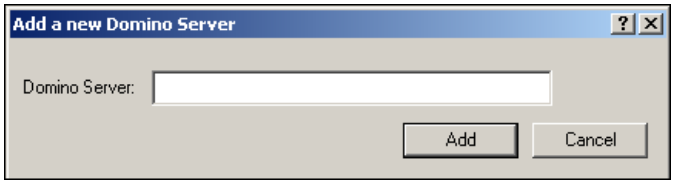
Note

Users must use the Web site to enable and set up Push.

Adding a New Domino Server (for Push Capability)

1. From the Domino Push panel, choose New.

   The Add a new Domino Server dialog box appears.



2. Type the name of the Domino server you want to enable for Push. A new dialog box appears.
3. Specify an ID file. The ID you specify must have permission to run unrestricted agents.

Note
There is no equivalent procedure for Microsoft Exchange. The Exchange server automatically notifies the Nokia Intellisync Mobile Suite server when there is a change.

Device Management/File Sync Tab

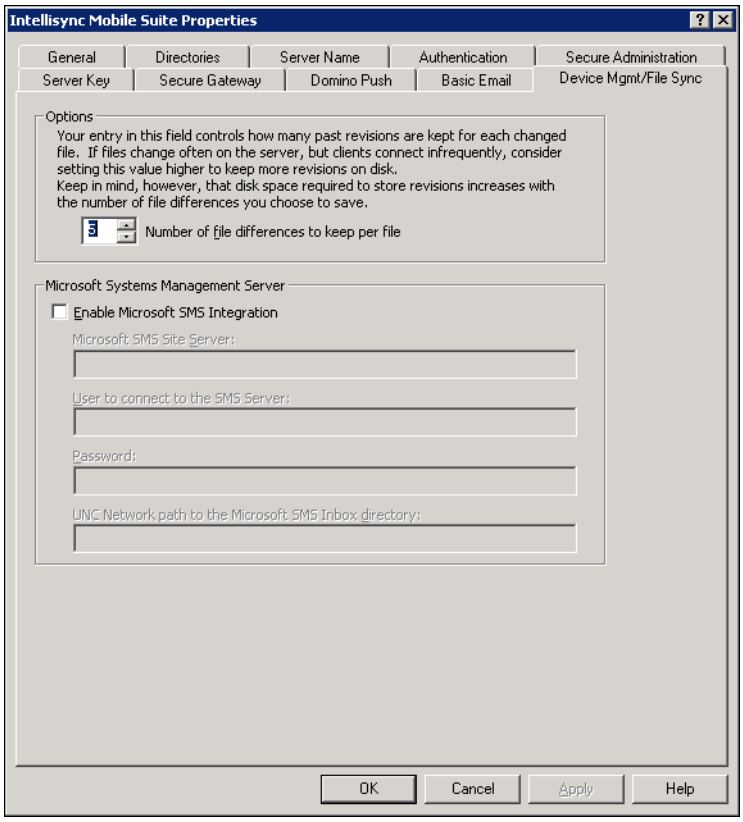
Set the number of file revisions to keep and enable SMS integration on the Device Management/ File Sync tab.

To view the Device Management/File Sync tab

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   The Nokia Intellisync Mobile Suite Properties dialog box appears.
3. Choose the Device Management/File Sync tab.

The Device Management/File Sync panel tab appears.

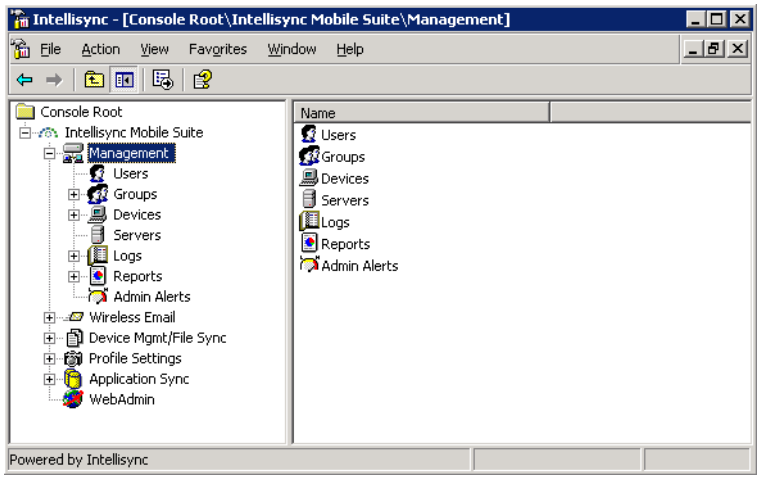


4. Use the following information to configure settings in the Options section.

Field	Description
Number of file differences to keep	Rather than storing complete copies of changed files, the system saves the differences that must be applied to bring an older version up-to-date. This value controls how many past revisions you keep for each file that changes. If your files change often on the server, but clients connect infrequently, consider setting this number higher to keep more revisions on disk. This approach helps to ensure that users receive the complete set of file revisions required to bring the client up to date. Keep in mind that the disk space you need to store file revisions increases with the number of file revisions you choose to save.
Microsoft System Management Server computer name to enable SMS integration	Select this option and enter SMS server name, user, password, and network path information. This allows you to import and distribute SMS packages to remote mobile users through the Nokia Intellisync product. These packages convert to software distribution packages.

Management Functions

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



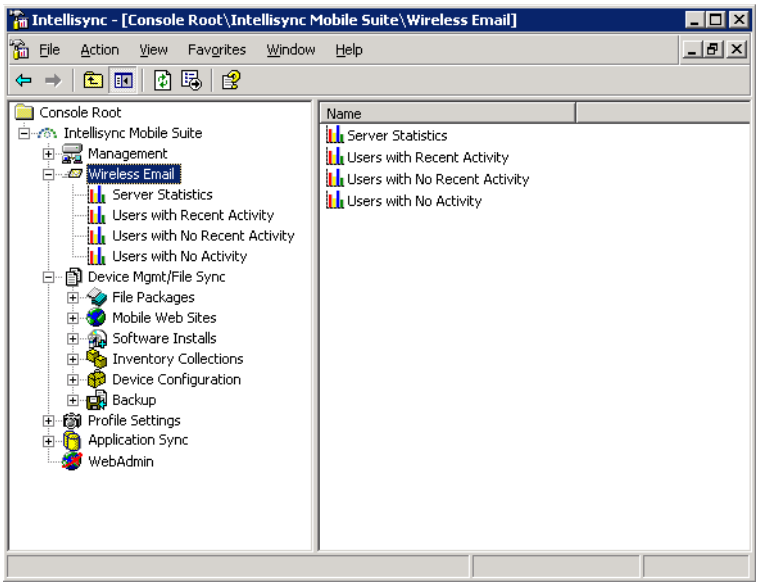
Use the Management control to complete the following tasks:

- Manage users and groups
- View a list of devices
- View logs
- Configure server clusters
- Use reporting functions
- Set up alerts (for Device 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.”

Nokia Intellisync Mobile Suite Products

Each product in Nokia Intellisync Mobile Suite has its own control in the Nokia Intellisync Mobile Suite control. The license key you entered at installation determines the products you see here. Depending on the products you have purchased, you may see several product controls.



The available products available are:

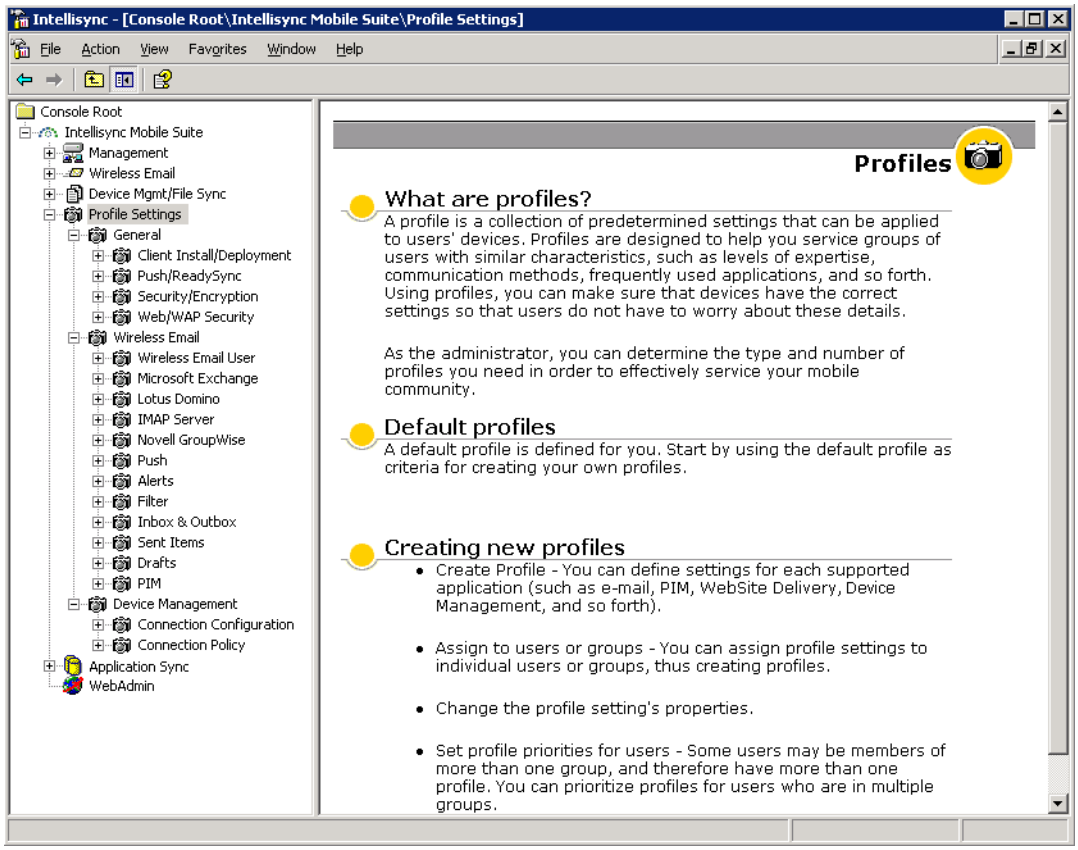
- Wireless Email
- Device Management
- File Sync
- Application Sync

Controls appear only for the products installed on your server.

For information on using Device Management or File Sync, refer to the *Nokia Intellisync Device Management and File Sync Administrator's Guide*. For more information on Application Sync, refer to the *Nokia Intellisync Application Sync Administrator's Guide*.

Profile Settings

Every Nokia Intellisync Mobile Suite product provides Profile Settings as a standard part of the Nokia Intellisync Mobile Suite control. You can use Profile Settings to create, modify, and manage user profiles, as the following example shows.



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

WebAdmin

WebAdmin is a Web-based Admin Console. WebAdmin allows you to manage information for your mobile community from the Web. You can complete many administrative tasks, including:

- Managing users, groups, and devices
- Viewing logs
- Running reports
- Managing administrators and tenants
- Managing settings for publications

This section provides a general overview of WebAdmin. You can access online help for more detailed instructions for completing the tasks.

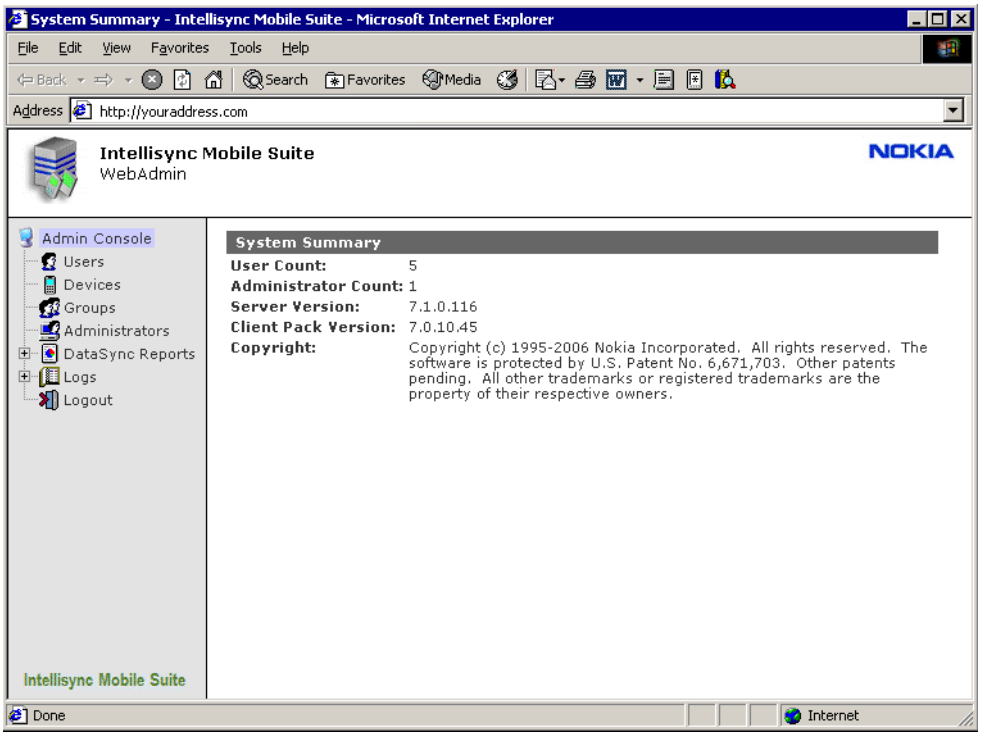
Accessing WebAdmin

Enterprise administrators can access WebAdmin from the MMC Admin Console as well as a Web browser.

To open WebAdmin

1. From the MMC Admin Console, right-click WebAdmin.
2. Choose Launch WebAdmin.

   The WebAdmin appears in a browser window.



Tenant administrators can access WebAdmin from a Web browser. The enterprise administrator provides the URL for tenant administrators. Detailed instructions on using WebAdmin are in the online help.

Configuring WebAdmin

The following nodes appear in WebAdmin:

- Users
- Devices
- Groups
- Publications
- Administrators
- Reports
- Logs
- Support

To view the Tenants node, you must configure WebAdmin to support tenants. For more information, refer to “Tenants” on page 51.

Users

From WebAdmin, select Users to view a list of all users. You can complete the following tasks for users:

- Adding a user
- Importing users
- Changing user information
- Changing a user’s device information
- Changing a user’s assigned groups
- Changing a user’s assigned publications
- Viewing a user’s activity
- Deleting a user

For more information, refer to “Working with Users” on page 53.

Devices

Select Device to access information such as the user, device status, and theft/loss protection settings. You can complete the following tasks for devices:

- Viewing device file information
- Viewing device hardware information
- Viewing device software information
- Changing device information
- Deleting a device

For more information, refer to “Devices” on page 67.

Groups

Select Groups to view a list of all groups. You also have access to more detailed group information including users, child groups, and subscribed publications. You can complete the following tasks for groups:

- Adding a group
- Adding a child group
- Changing group information
- Changing a group's assigned users
- Changing a group's subscribed publications
- Deleting a group

For more information, refer to "Working with Groups" on page 63.

Publications

Select Publications to view a list of publications. You also have access to individual publication information such as subscribed users and groups. You can complete the following tasks for publications:

- Changing publication information
- Subscribing users to a publication
- Subscribing groups to a publication

For more information, refer to the *Device Management/File Sync Administrator's Guide*.

Administrators

Select Administrators to access individual administrator information such as status, time zone, and language. You can complete the following tasks for administrators:

- Adding an administrator
- Changing administrator information
- Deleting an administrator

Reports

Select Reports to view a list of reports. The Memory Usage Report displays user, memory, and asset collection information for a selected device type. The Carrier Info Report displays carriers and device counts. The Application Report displays application and device count information for a selected device type. For more information, refer to "Reports" on page 72.

Logs

Select Logs to view a list of logs. The Audit Trail Log displays a description of Admin Console changes within selected date and time parameters. The User Activity Log displays user activity information within selected date and time parameters. For more information, refer to "Log Files" on page 71.

Tenants

The Tenant node does not appear in WebAdmin by default. For the server to support multiple tenants for hosted service providers, complete the following steps.

To configured the server for multiple tenants

1. On the computer on which the server is installed, open a browser window.
2. Enter `localhost/diag` in the address bar, and choose Go.

   The System Info And Diagnostics page appears.
3. Choose General.
4. In the Add Property field, enter `ShowMultitenantUI` and set the value to `1`.
5. Exit the browser window.
6. Restart the server to activate the setting.

The Tenants control allows you to view a list of tenants or select an individual tenant to view more detailed information such as the number of users, groups, publications, and administrators. You can complete the following tasks for tenants:

- Log in as a tenant
- Add a tenant
- Change tenant information
- Assign administrators to a tenant
- Assign groups to a tenant
- Assign publications to a tenant
- Add users to a tenant
- Delete a tenant

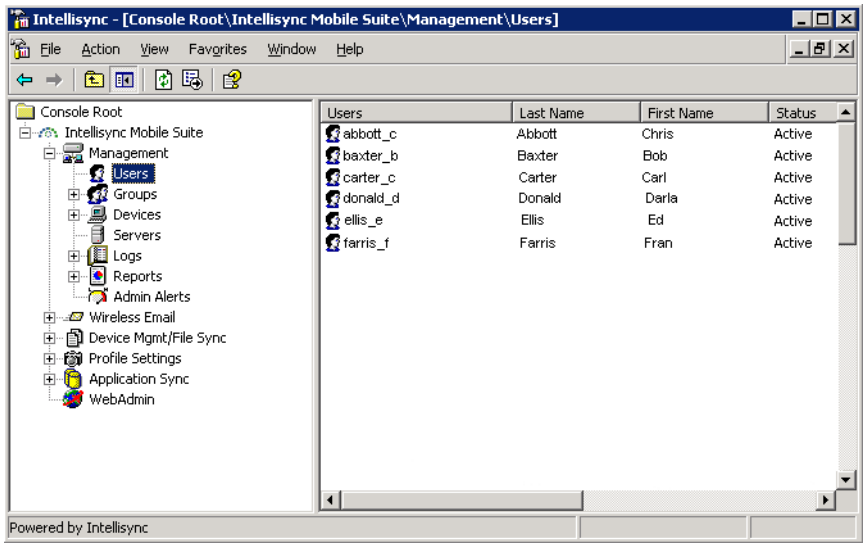
3 Using Management Tools

The Management control gives you easy access to functions that apply to the entire suite, such as managing users and groups and using logs and reports. Expand the Management control to access the following controls:

- Users
- Groups
- Devices
- Servers
- Logs
- Reports
- Admin Alerts (for Device Management or File Sync only)

Working with Users

All Nokia 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, as the following example shows.



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:

- Adding a new user
- Importing and synchronizing users
- Changing a user's group memberships
- Assigning and editing user profiles
- Deleting a user
- Using the Properties dialog box to manage user information

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

Adding a New User

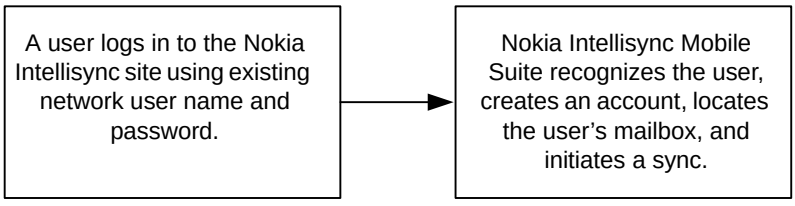
Depending on how your system is set up, you can add new users to your system through the Nokia Intellisync Mobile Suite control.

The method you are using to authenticate users determines the way in which you add new users. For example, if you are using Windows NT or Domain 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 Nokia Intellisync Authentication, then add or import new users using the Nokia Intellisync Mobile Suite control.

Adding Users Through Auto Discovery

If you are using Windows NT Domain Authentication, there is no need to manually add users through the Nokia 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 user discovery appear in the list of users along with all other user accounts.

Figure 5 Overview of User Discovery Process



User discovery is enabled by default.

To change the user discovery setting

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.
3. Choose the Authentication tab.
4. Select or clear the Allow Users To Be Discovered And Created At Connect Time check box.

For more information about Windows NT Domain Authentication, see Chapter 7, "Authenticating Users."

Adding Users Through the Admin Console

To add users in the Admin Console

1. From the console tree, select Management, and then select Users.
2. Choose Action > Create User.
3. Add a unique user name, password, and optional information as needed.

For more information on completing this task, choose Help.

The Nokia 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 Nokia Intellisync Mobile Suite control are set up for Nokia 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 Windows NT, Domino authentication, or GroupWise authentication, Nokia Intellisync Mobile Suite adds new users when they connect for the first time. Therefore, do not manually add users through the Nokia Intellisync Mobile Suite control.

Importing and Synchronizing 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 the following sources:

- Text file
- Windows NT or Windows 2000 domains
- Active Directory/LDAP

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.

To import users from a text file

1. Prepare a text file containing user information. (The text file should have one user ID per line.)
2. In the console tree, select Management, and then select Users.
3. Choose Action > Import Users from File.
4. Locate the text file and select 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, choose Help.

Intellisync Mobile Suite 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 password 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=<followed by the password for this user>
- $description=<followed by some descriptive text about this user>
- $firstname=<followed by the user's first name>
- $lastname=<followed by the user's last name>
- $addtogroup=<followed by the group name to which the user should be a member>
- $active=<followed by 0 or 1, where 0 indicates inactive and 1 indicates active>
- $alertdevice=<followed by phone, pager, or email address>
- $alertphonenumber=<followed by the phone number of the alert device>
- $alertemailaddr=<followed by the email address to receive alerts>
- $alertcarrier=<followed by Verizon, Sprint, AT&T Wireless, Alltel, T-Mobile, or Cingular>
- $emailAddress=<followed by the user's email address>

- $language=<followed by two-character country code. Valid entries are EN (English), FR (French), ES (Spanish), DE (German), JA (Japanese)>
- $Tenant=<followed by the tenant name to which the user should be added. This parameter is used for importing users through the WebAdmin. This token is honored only when a non-Tenant administrator is logged in. The token allows the hosted administrator to import users and automatically assign the users to tenants.>
- $timezone=<followed by timezone specification>
- $authtype=<followed by -1 for NT; 0 for IMS authentication>
- $sync=<followed by 1. This triggers a sync after configuration>
- $serverdevice=<followed by Domino, Exchange, GroupWise, IMAP, or XML,<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 = Domino:

  $dominousername=<followed by the Domino user name. The domino user name may be canonical or abbreviated. This parameter is required for courier access. It is not used otherwise.>

  $dominoidfile=<followed by the path to the user's ID file. This parameter is required for upload ID file access. It is not used otherwise.>

  $dominopassword=<followed by the password for the user's ID file. This parameter is required for upload ID file access. It is not used otherwise.>

- If $serverdevice = Exchange:

  $exchangeserver=<followed by the exchange server>

  $exchangemailbox=<followed by the exchange mailbox, which can be specified using "firstname lastname" or the alias (the text before the @ in the primary email address)>

  You have to use courier access to configure Exchange.

- If $serverdevice= GroupWise:

  $GWServer=<followed by the GroupWise server>

  $GWPort=<followed by the GroupWise port number>

  $GWUuid=<followed by the GroupWise user unique ID>

  $GWDisplayName=<followed by the GroupWise user full name>

  $GWUser=<followed by the GroupWise user name>

  $GWPassword=<followed by the GroupWise user password. This parameter is not required for trusted application access>

- If $serverdevice = IMAP:

  $IMAPServer=<followed by the IMAP server name>

  $IMAPUser=<followed by the IMAP user ID>

  $IMAPPassword=<followed by the IMAP password for the user>

  $IMAPInboxFolderName=<followed by the IMAP Inbox folder name on the server>

  $IMAPDraftsFolderName=<followed by the IMAP Drafts folder name on the server>

  $IMAPSentItemsFolderName=<followed by the IMAP Sent Items folder name on the server>

- If $serverdevice = XML,<ID>:

  $XMLUser=<followed by the XML user ID>

  $XMLPassword=<followed by the XML password for the user>

  $XMLCompany=<followed by the company name on the server>

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

Time Zone Reference

For this time zone	Enter this information in import file
A	
• “Abu Dhabi, Muscat”	• “Asia/Muscat”
• “Adelaide”	• “Australia/Adelaide”
• “Alaska”	• “America/Anchorage”
• “Almaty, Novosibirsk”	• “Asia/Novosibirsk”
• “Amsterdam, Berlin, Rome, Vienna”	• “Europe/Berlin”
• “Arizona”	• “America/Phoenix”
• “Astana, Dhaka”	• “Asia/Dacca”
• “Athens, Istanbul, Minsk”	• “Europe/Athens”
• “Atlantic Time (Canada)”	• “America/Halifax”
• “Auckland, Wellington”	• “Pacific/Auckland”
• “Azores”	• “Atlantic/Azores”

For this time zone	Enter this information in import file
B	
• “Baghdad”	• “Asia/Baghdad”
• “Baku, Tbilisi, Yerevan”	• “Asia/Yerevan”
• “Bangkok, Hanoi, Jakarta”	• “Asia/Bangkok”
• “Beijing, Chongqing, Hong Kong, Urumqi”	• “Asia/Hong_Kong”
• “Belgrade, Bratislava, Budapest, Prague”	• “Europe/Prague”
• “Bogota, Lima, Quito”	• “America/Bogota”
• “Brasilia”	• “America/Sao_Paulo”
• “Brisbane”	• “Australia/Brisbane”
• “Brussels, Copenhagen, Madrid, Paris”	• “Europe/Paris”
• “Bucharest”	• “Europe/Bucharest”
• “Buenos Aires, Georgetown”	• “America/Buenos_Aires”
C	
• “Cairo”	• “Africa/Cairo”
• “Calcutta, Chennai, Mumbai, New Dehli”	• “Asia/Calcutta”
• “Canberra, Melbourne, Sydney”	• “Australia/Sydney”
• “Cape Verde Is.”	• “Atlantic/Cape_Verde”
• “Caracas, La Paz”	• “America/Caracas”
• “Casablanca, Monrovia”	• “Africa/Casablanca”
• “Central America”	• “America/El_Salvador”
• “Central Time (US & Canada)”	• “America/Chicago”
• “Chihuahua, La Paz, Mazatlan”	• “America/Mazatlan”
D	
• “Darwin”	• “Australia/Darwin”
• “Dublin, Edinburgh, Lisbon, London”	• “Europe/London”
E-F	
• “Eastern Time (US & Canada)”	• “America/New_York”
• “Ekaterinburg”	• “Asia/Ekaterinburg”
• “Fiji, Marshall Is.”	• “Pacific/Fiji”
G	
• “Greenland”	• “America/Godthab”
• “Guam, Port Moresby”	• “Pacific/Guam”
H	
• “Harare, Pretoria”	• “Africa/Harare”
• “Hawaii”	• “Pacific/Honolulu”
• “Helsinki, Tallinn”	• “Europe/Helsinki”
• “Hobart”	• “Australia/Hobart”

For this time zone	Enter this information in import file
I-J	
• “Indiana (East)”	• “America/Indianapolis”
• “International Date Line West”	• “Pacific/DateLineWest”
• “Irkutsk, Ulaan Bataar”	• “Asia/Irkutsk”
• “Islamabad, Karachi, Tashkent”	• “Asia/Karachi”
• “Jerusalem”	• “Asia/Jerusalem”
K	
• “Kabul”	• “Asia/Kabul”
• “Kathmandu”	• “Asia/Katmandu”
• “Krasnoyarsk”	• “Asia/Krasnoyarsk”
• “Kuala Lumpur, Singapore”	• “Asia/Singapore”
• “Kuwait, Riyadh”	• “Asia/Kuwait”
M	
• “Mexico City”	• “America/Mexico_City”
• “Mid-Atlantic”	• “Atlantic/Mid”
• “Midway Island, Samoa”	• “Pacific/Pago_Pago”
• “Moscow, St. Petersburg, Volgograd”	• “Europe/Moscow”
• “Mountain Time (US & Canada)”	• “America/Denver”
N	
• “Nairobi”	• “Africa/Nairobi”
• “Newfoundland”	• “America/St_Johns”
• “Noronha”	• “America/Noronha”
• “Nuku'alofa”	• “Pacific/Tongatapu”
O-P-R	
• “Osaka, Sapporo, Tokyo”	• “Asia/Tokyo”
• “Pacific Time (US & Canada); Tijuana”	• “America/Los_Angeles”
• “Perth”	• “Australia/Perth”
• “Rangoon”	• “Asia/Rangoon”
S	
• “Santiago”	• “America/Santiago”
• “Sao Paulo”	• “America/Sao_Paulo”
• “Sarajevo, Sofija, Warsaw, Zagreb”	• “Europe/Warsaw”
• “Saskatchewan”	• “America/Regina”
• “Seoul”	• “Asia/Seoul”
• “Solomon Is.”	• “Pacific/Guadalcanal”
• “Sri Jayawardenepura”	• “Asia/Colombo”
T	
• “Taipei”	• “Asia/Taipei”
• “Tehran”	• “Asia/Tehran”

For this time zone	Enter this information in import file
V-W-Y	
• “Vladivostok”	• “Asia/Vladivostok”
• “West Central Africa”	• “Africa/Algiers”
• “Yakutsk”	• “Asia/Yakutsk”

Importing Windows NT or Windows 2000 Users

If the users you want to add are registered Windows NT or Windows 2000 users, you can import and synchronize the users into the Nokia Intellisync Mobile Suite control.

To import Windows NT or Windows 2000 users

1. From the console tree, select Management, and then select Users.
2. Choose Action > Import/Synchronize User List > NT Domain Users.
3. Follow the prompts on the Import/Synchronize Users wizard.

For more information on completing these tasks, choose Help.

The Nokia Intellisync Mobile Suite control creates the user IDs in the <domain>\<user name> format. The users are now part of the All Users Group and the New Users Group. Use the Properties dialog box to enter additional information for each user.

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

The new users are not assigned to a device type. When a user connects with a specific device, that device type is registered for the user.

Importing Active Directory/LDAP Users

You can import and synchronize users that exist on an LDAP directory such as Microsoft’s Active Directory or the Netscape/Sun iPlanet directory server.

To import Active Directory/LDAP users

1. From the console tree, select Management, and then select Users.
2. Choose Action > Import/Synchronize User List > Active Directory/LDAP Users.
3. Follow the prompts on the Import/Synchronize Users wizard.

The Nokia Intellisync Mobile Suite control creates the user IDs and assigns the IDs to the All Users Group and New Users Group. Use the Properties dialog box to enter additional information for each user.

Adding users this way allows you to use NT Domain Authentication by default. You can view and change the method for validating a user on the General tab of the user’s properties.

The new users are not assigned to a device type. When a user connects with a specific device, that device type is registered for the user.

Subscribing Users to Group

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

To add or modify a user's group subscriptions

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

Assigning/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 a profile, the Assign Profiles option appears.

Note
Users with no profile, either individually or through groups, automatically receive a profile by default. See "Default Profile Settings" on page 78.

To assign or edit a user profile

1. From the console tree, select Management, and then select Users.
2. In the Details pane, select the user ID to which you want to assign or edit profiles.
3. Choose Action menu > Assign Profiles or Edit Profiles.
4. Use the tabs and lists to select profiles for each of the user's devices.
5. Choose OK.

Deleting a User

You can delete user accounts that you no longer need. When you delete a user, Intellisync Mobile Suite deletes the information across all licensed Intellisync Mobile Suite products.

To delete a user

1. From the console tree, select Management, and then select Users.
2. In the Details pane, select the user ID you want to delete.
3. Choose Action > Delete.

   A confirmation message appears.
4. Choose Yes.

Managing User Information

After you create a user account, use the Properties dialog box to add or change user information. To make several changes for one user, you may 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

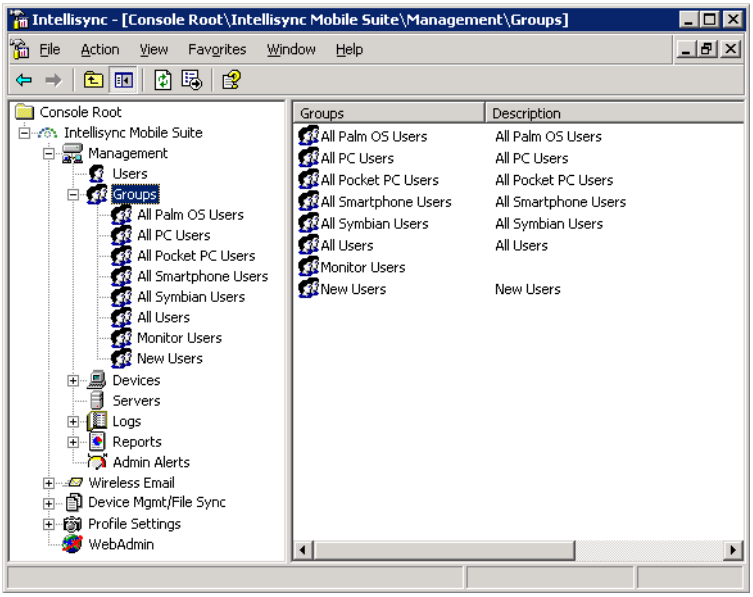
To use the Properties dialog box

1. From the console tree, select Management, and then select Users.
2. In the Details pane, select the user ID.
3. Choose Action > Properties.

Working with Groups

You can create groups and assign users to the groups. You can import groups from Windows NT or other defined LDAP source. 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.



This section contains the following information for working with groups:

- Creating a Group
- Importing and Synchronizing Groups (from Windows NT or an Active Directory/LDAP source)
- Adding or Removing Users from a Group
- Assigning/Editing Group Profiles
- Deleting a Group
- Managing User Information

Creating a Group

To add a group

1. From the console tree, select Management, and then select Groups.
2. Choose Action > Create Group.
3. Type a group name and a description.
4. Choose OK.

For more information about creating groups, refer to the online help.

Note
You cannot remove a user from the All Users group.

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 Nokia Intellisync Mobile Suite control. This eliminates the need to create and manage groups in two areas.

To import Windows NT or Windows 2000 groups

1. From the console tree, select Management, and then select Groups.
2. Choose Action > Import/Synchronize Groups > NT Domain Groups.
3. Follow the prompts on the Import/Synchronize Groups wizard.

Active Directory/LDAP Groups

To import Active Directory/LDAP groups

1. From the console tree, select Management, and then select Groups.
2. Choose Action > Import/Synchronize Groups > Active Directory/LDAP Groups.
3. Follow the prompts on the Import/Synchronize Groups wizard.

Adding or Removing Users from a Group

To add or delete users from a group

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

Note
You cannot remove a user from the All Users group.

Assigning/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.

Note
Groups with no profile automatically receive a profile by default. See "Default Profile Settings" on page 78.

To assign or edit profiles for a group

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

Deleting a Group

To delete a group

1. From the console tree, select Management, and then select Groups.
2. In the Details pane, select the name of the group you want to delete.
3. Choose 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.

Managing Group Information

After creating a group, you can use the Properties dialog box to add or change information about the group. To make several changes for one group, you may 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

1. From the console tree, select Management, and then select Groups.
2. In the Details pane, select the name of the group.
3. Choose Action > Properties.
4. Change the values as necessary.

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

Devices

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

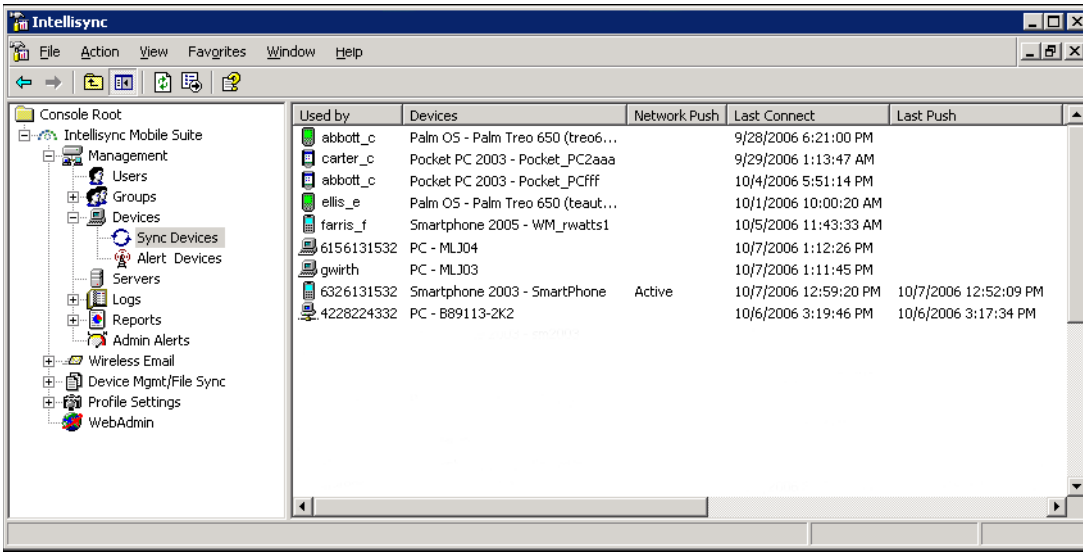
- Sync Devices
- Alert Devices

To view the status of a device

1. From the console tree, select Management, and then select Devices.

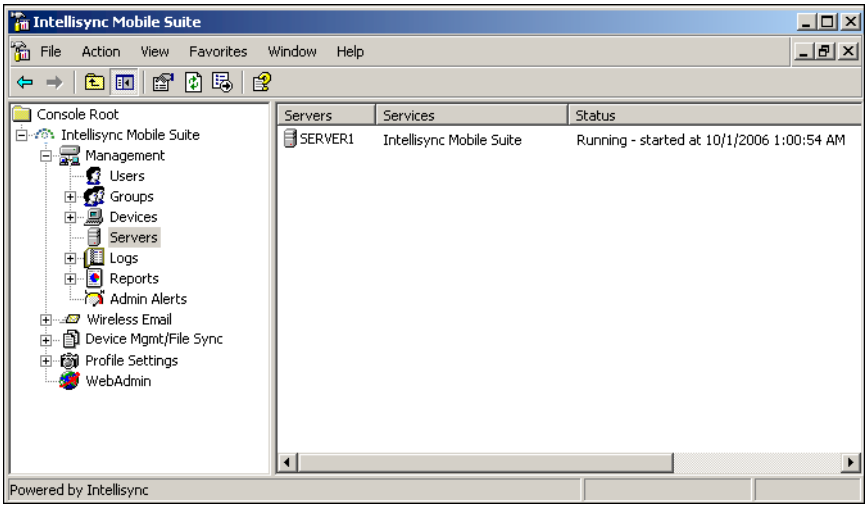
   The device types appear in the Details pane.
2. Select a device type.

The status appears in the Details pane.



Servers

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



Note
You must contact an Nokia 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 may cause irreparable damage to your system.

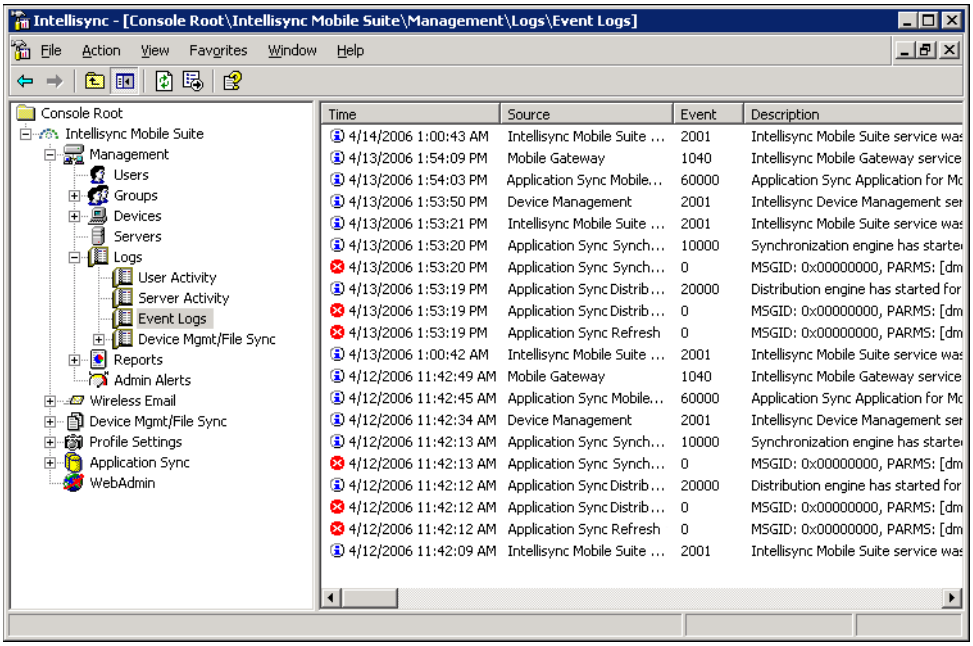
Logs

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.

To view logs

1. From the console tree, select Management > Logs.
2. Select the type of log you want to view.

   The log information appears in the Details pane.



Log Levels

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

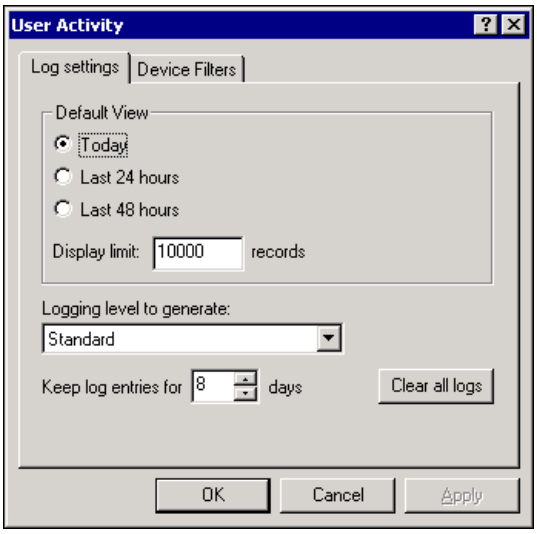
- **Minimum.** Shows only warnings and error messages.
- **Standard.** Shows general information messages and minor warnings, in addition to serious warnings and error messages.
- **Verbose.** Shows all log messages.

Note

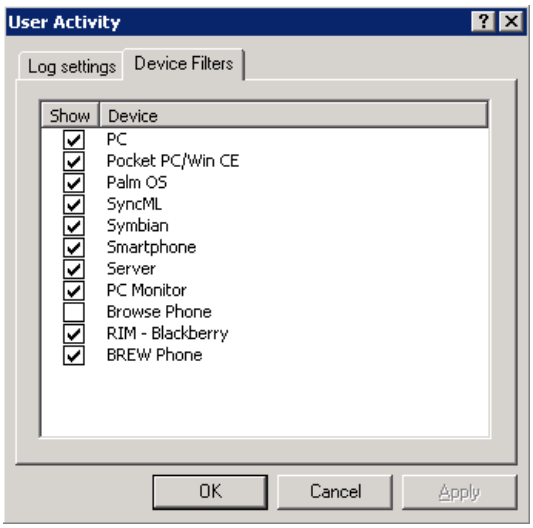
For the User Activity summary, you can view only the message detail level you elected to capture from the client users (or a less selective level). For example, if client logging is set to Standard, then Verbose messages are not captured.

Changing Log Defaults and Settings

The User Activity and Server Activity logs include a Settings button to change the default view or set how long you want to keep log entries on the system. The following example shows the Log settings panel on the User Activity Settings dialog box.



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



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.

Available Logs

The following logs are available.For more information on using logs, refer to the online help.

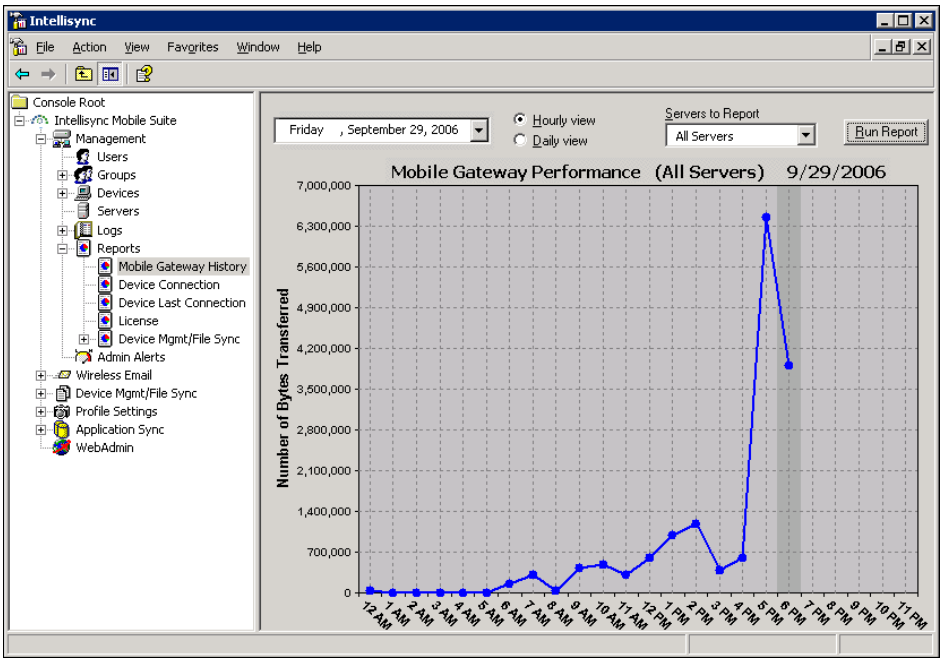
Log	Description
User Activity	Displays connection information on a user-by-user basis. You can select the user, start date, end date, and time.
Server Activity	Displays server activity for the start date, end date, and time you specify. Unlike the Event Logs, which display log entries for the computer 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 Nokia Intellisync Mobile Suite server you select. You can see start and stop times for services, as well as critical error information.
Device Mgmt/File Sync Logs	Contains information specific to Device Management and File Sync.

Log Files

Log files are stored in the Intellisync\Log directory, depending your system setup. If you are having problems with your system, an Nokia Intellisync support engineer may ask you to send these files for analysis.

Reports

You can use reports to review information about your system. After you provide the appropriate input data, choose Run Report to generate an on-screen report, as the following example shows. For more information on using reports, refer to the online help.



Available Reports

You can run the following reports:

- Mobile Gateway History
- Device Connection
- Device Last Connection
- License
- Device Mgmt/File Sync

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.

Device Last Connection

The Device Last Connection report provides a list of the latest connection dates and times for devices. User and date filters are available.

License

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

Device Mgmt/File Sync

If Device Management or File Sync is part of your system, the following reports are available from Nokia Intellisync Mobile Suite control.

- Staged Files
- Publication Status
- Scheduled Publication Status
- Application Summary
- Hardware Summary

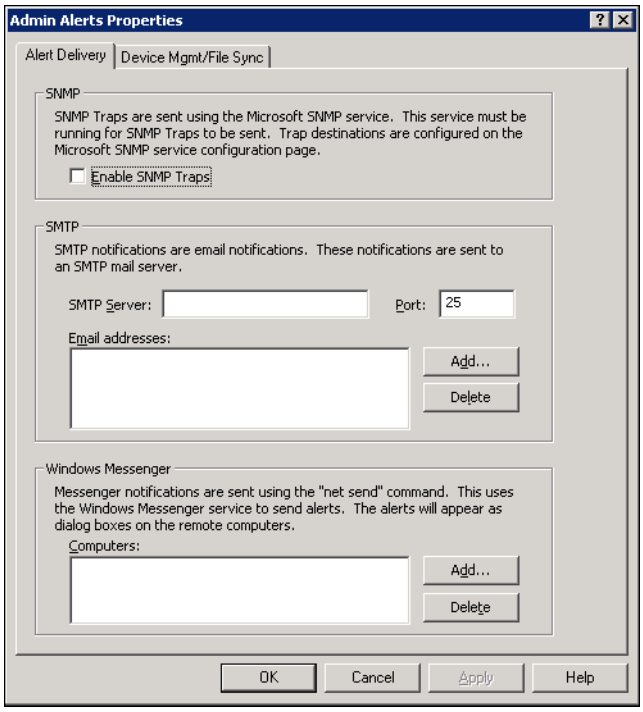
Admin Alerts

Admin Alerts is a feature of Device Management and File Sync. Admin alerts appear in Nokia Intellisync Mobile Suite control only if these products are part of your system.

To configure alerts

1. From the console tree, select Management, and then select Admin Alerts.
2. Choose Action > Configure Alerts.

The Admin Alerts dialog box appears.



For more information on Admin Alerts, refer to the Device Management and File Sync online help.

Accessing a Device Remotely

Use this option to access a user's device remotely when you want to troubleshoot a problem or guide the user through complicated procedures. Using the remote control feature, you can see the client screens on in real time just as the user sees the screens. Likewise, the user sees the result of any actions you perform on the device from your remote location

Before You Begin

Consider the following important information before you begin.

- Before taking control of a user's device, consider letting the user know you will be accessing the device.
- If you are taking control of a user's laptop or PC, the user have Java Plug-in version 1.5 or higher installed.
- If you or the user disconnect before finishing the intended session, return to step 1 in this procedure to reconnect.

To access a user's device remotely

1. From the console tree, choose Management > Devices.
2. Select the device you want to access.

   The device's page appears.
3. Choose Remote Control.

   The user sees the text message, "Your administrator is requesting a remote control connection. Do you accept? yes no"

   After the user receives a message on the device and chooses yes, your screen reveals a skin representing the user's device interface and hardware controls.

4 Profile Settings

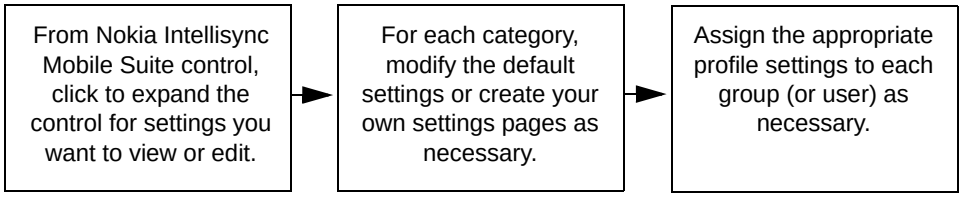
Profiles are collections of general and application settings that define how Nokia Intellisync Mobile Suite is set up for a specific user or group. With Profiles, you can define settings for options such as ReadySync, security/encryption, Web/WAP security, email, calendars, contacts, file delivery, and 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 Nokia 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
- Delete profile settings

Figure 6 Process Overview: Working with Profile Settings



Note
You do not have to make changes to profile settings for users to connect and synchronize with Nokia Intellisync Mobile Suite. The default profile settings automatically apply to each user and group. You may want to see how your system operates with the default settings before making any changes.

Managing 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 Nokia Intellisync Mobile Suite control.

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 Nokia Intellisync Mobile Suite product installed on your server. Expand these options to see the associated profile settings.

Default Profile Settings

Several profile settings are set up for you in advance, and some default settings may be sufficient for you. However, if you want to create new profile settings, you can use the default settings as a starting point.

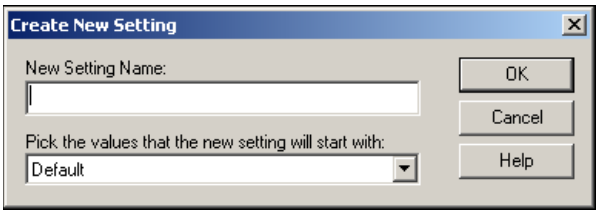
Adding a New Profile Based on an Existing Profile

To add a new profile setting based on an existing profile

1. Choose Action > Create New Setting.

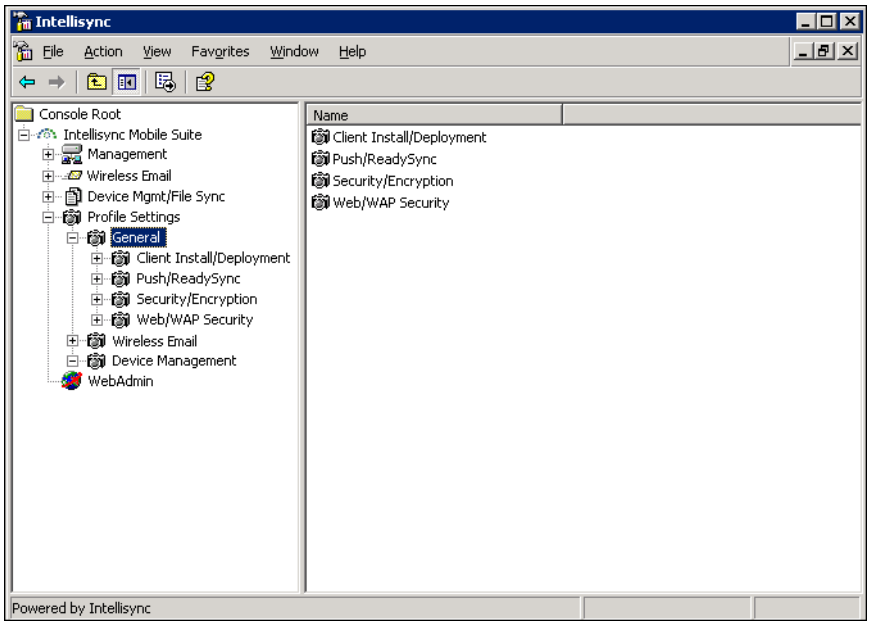
   The Create New Setting dialog box appears.

2. Type a name for the new setting.
3. From the list, choose an existing profile setting whose values are similar to those for the setting you are creating.



General Settings

The General control includes settings that are not application specific, but apply to the entire suite.



Configuring Client Install/Deployment Settings

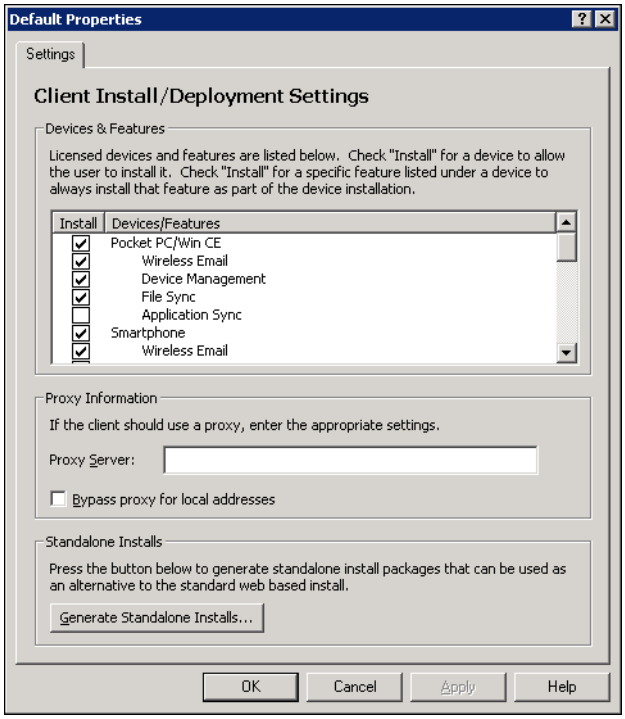
Client Install/Deployment profile settings allow you to create a set of Nokia Intellisync Mobile Suite applications for various installation and deployment profiles. The applications you specify become part of every device installation for users assigned to a particular profile.

To configure Client Install/Deployment settings

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

   The Client Install/Deployment Settings Properties dialog box appears.

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



6. Choose Generate Standalone Installs 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 about creating and assigning these profiles, refer to the online help.

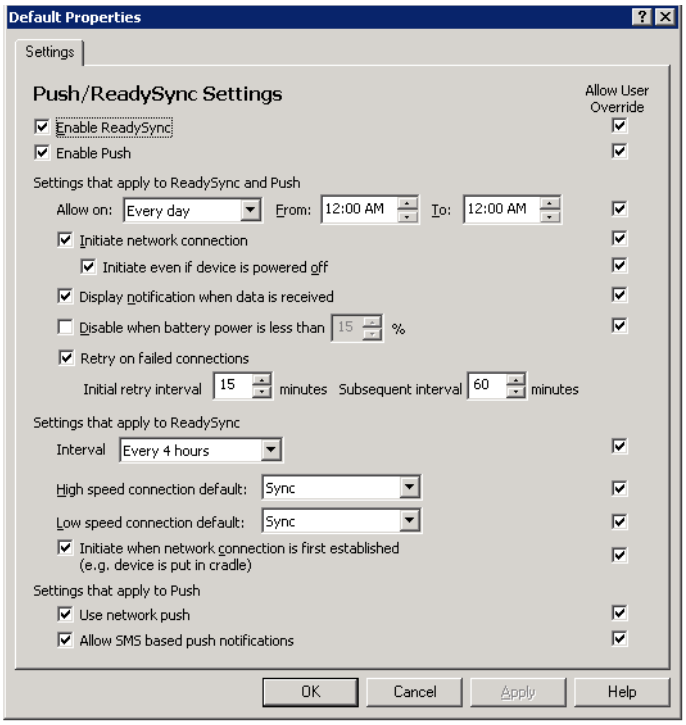
Configuring ReadySync Settings

ReadySync Settings profile settings allow you 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 email messages on their devices soon after the email arrives on the server.

To configure ReadySync settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > General > Push/ReadySync.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

The Push/ReadySync Settings Properties dialog box appears.



5. Enter information for the following fields and click OK.

Field	Description
Enable ReadySync/Push	
Enable ReadySync	Select this option to enable the ReadySync feature or clear the check box to disable.
Enable Push	Select this option to enable the Push feature or clear the check box to disable.

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

Settings That Apply To ReadySync And Push	
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.

Field	Description
Initiate Network Connection	If you enable this feature, the device dials for a connection when a ReadySync session begins. Select or clear the check box to enable or disable the feature. Initiate Even If Device Is Powered Off—This option is available only 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 clear 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	Initial Retry Interval <x> minutes Subsequent Interval <x> minutes
Settings That Apply Only To ReadySync	
Interval	Select the frequency with which you want ReadySync to connect. Options range from every 10 minutes to every 24 hours. • Every 10 minutes • Every 15 minutes • Every 20 minutes • Every 30 minutes • Every hour • Every 2 hours • Every 4 hours • Every 12 hours • Every 24 hours
High-Speed Connection Default	Select Sync, SyncXpress, or Do Not Sync. 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 Do Not Sync.
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.
Settings That Apply Only To Push	
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.

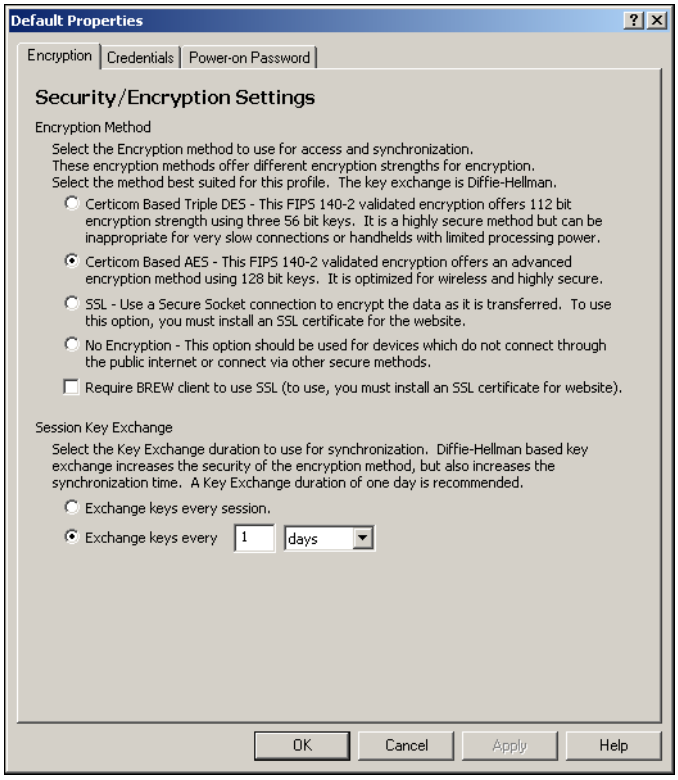
Configuring Security/Encryption Settings

Security/Encryption profile settings allow you to define the encryption method you want to use to access the server, synchronize data, and store client authentication credentials. The methods have varying levels of security; therefore, you can select the method best suited for a particular user or group. The key exchange is Diffie-Hellman.

To configure Security/Encryption settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > General > Security/Encryption.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The Security/Encryption Settings Properties dialog box appears with the Encryption panel open.



5. Enter information for the following fields and click OK.

Field	Description
Certicom Based Triple DES	FIPS 140-2 validated encryption. This highly secure method has 112-bit encryption strength using three 56-bit keys. Nokia 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 BREW Client To Use SSL	Select this option to require BREW devices to use SSL. If you enable this option, your Web site must have an SSL certificate.

6. Select the frequency of key exchange to use for synchronization. The Diffie-Hellman key exchange offers increased security, but it increases the synchronization time.

   By default, the recommended one-day duration is selected. You can select from the following.

   - Exchange keys every session
   - Exchange keys every <number> <days, minutes, hours>

Configuring User Credentials

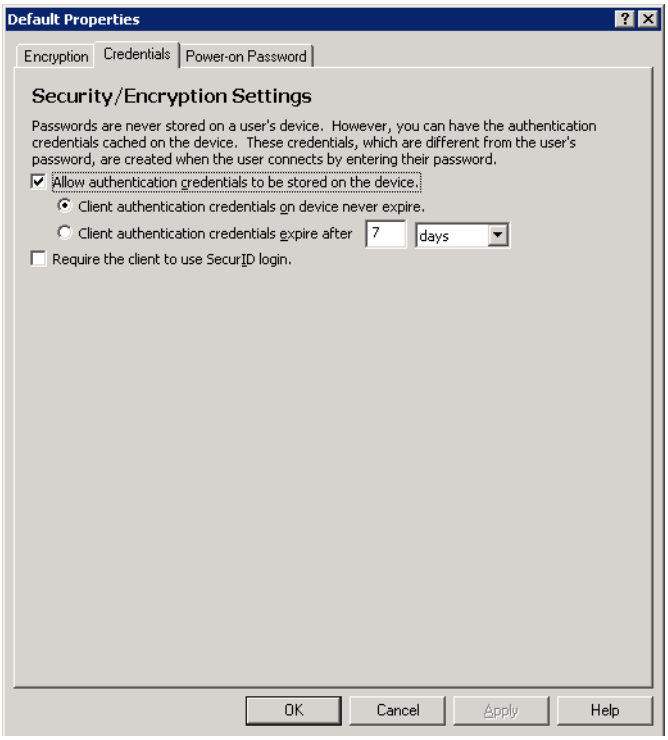
Nokia Intellisync Mobile Suite does not store user passwords on the device. However, you can use the Password panel to have authentication credentials cached on the device. These authentication credentials are different from the user's password and are created when the user connects by entering a password.

To configure credentials

1. Access Security/Encryption Settings properties.

   For more information, see "To configure Security/Encryption settings" on page 83.

2. Choose the Credentials tab.



3. Enter information for the following fields and click OK.

Field	Description
Allow Authentication Credentials To Be Stored On The Device	Select or clear the check box to enable or disable this feature.
Client Authentication Credentials On The Device Never Expire	This option is available only if you select the above option. Select this option to store authentication credentials on the user's device indefinitely.
Client Authentication Credentials Expire After <x> <minutes, hours, or days>	This option is available only 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 device.
Require The Client To Use SecurID Login	Select this option to add an additional layer of security. When this option is selected, each user is required to have a SecurID login. You must have an existing SecurID server in order to require SecurID for users.

Configuring Power-on Password Settings

To increase security on a user's device, you can configure a user's device to lock after it remains inactive for a specified period of time, requiring the user to enter a Power-on Password before regaining access to the device.

Note
This option is available only for Pocket PC, Smartphone, and Palm devices, and only if a licensed copy of Device Management exists on the console.

The following is an example of configurable user restrictions on a locked device.

User can...	User cannot...
Accept an incoming call using DTMF tones.	Synchronize the device.
Make certain outgoing calls (configured by the administrator), described in "To configure calling on a locked device" on page 88.	Access or view any screens other than the password screen.
Enter the latest user-selected Power-on Password or administrator-generated random password.	Make calls other than what is configured.

To configure power-on password settings

1. Access Security/Encryption Settings properties. For more information, see "To configure Security/Encryption settings" on page 83.
2. Choose the Power-on Password tab, then select Enforce Power-on Password. The screen enters edit mode.
3. Select the password type you want to enforce.

Field	Length	Restrictions
Simple 4 Numeric Character Password	4 exactly	Numerical digits only; no letters, punctuation, or symbols.
*Simple 4 Alphanumeric Character Password	4 exactly	Numerical digits and letters only; no punctuation, or symbols. Letters are case sensitive.
*Strong 5-40 Alphanumeric Character Password	5 through 40	Numerical digits and letters only; no punctuation or symbols. Can include all numbers or all letters. Letters are case sensitive.

Field	Length	Restrictions
*Strong 8-40 Multi-Character Password	8 through 40	Must contain at least one of each of the following and then no other character types: • lowercase letter • uppercase letter • numerical digit • - ( ) ! ? . : / or + Letters are case sensitive.

Note

Passwords are not restricted except as outlined in the previous table. For example, a user can reuse previous passwords, enter passwords using all the same digits, such as 1111, or numbers all in a sequence, such as 1234.

User-generated passwords do *not* expire, forcing users to change a password after a set interval. The password remains valid until a user changes the password or contacts the administrator to receive a new, randomly generated password.

The rows marked with * indicate features used only by Pocket PC, Smartphone, or Palm platforms.

4. In the “Prompt If Device Unused For” field, choose the amount of idle time before the user’s device displays the Power-on Password screen.

Time interval	Description
0 minutes	Locks only when • user powers off the device manually or • the device is configured to turn off automatically to save power.
1 minute 5 minutes 15 minutes 30 minutes 1 hour 90 minutes 2 hours 12 hours 24 hours	Displays the Power-on Password screen after this time interval passes.

5. Do one or more of the following options:
   - If you want to automatically generate a random password for a user who forgets the power-on password, see "To generate a random password" on page 88.
   - If you want to allow users to make restricted outgoing calls, see "To configure calling on a locked device" on page 88.
   - To save all configurations, choose Apply and then OK.

To generate a random password

You can generate a random password for a user. The random password has the same characteristics as the power-on password defined in step 3 on page 86.

- To generate a random password, go to the Power-on Password panel and check the box labeled Create A Random Safe Password For Users Who Forget Their Device's Password.
- To generate a random password that sets automatically at defined intervals, go to the Power-on Password panel and check the box labeled Change Random Password Every <time interval>, and enter the time interval <in hours, days, or weeks>.
- Choose Apply and then OK.

To configure calling on a locked device

You can configure the device so that within certain restrictions, a user can make an outgoing phone call with the device locked. For example, you can restrict the user to dial a limited number of digits to allow only three-digit emergency calls such as 911. You can also allow the user to dial only specific phone numbers, such as the number to call if they find the phone.

1. To restrict the number of digits a user can enter, in the Allow Dialing for <number> Digit Calls to be Dialed, enter one of the following:

Number	Device allows the user to enter the following...
3 through 10	Only the number of digits specified.
Any	Any number of digits.

2. To allow the user to dial only specific phone numbers, under Specific Numbers Allowed to be Dialed While Device is Locked, choose Add and type a description for the number and the phone number allowed, including area code. Do not enter any spaces or punctuation in the phone number.
3. Choose Apply and then OK.

Note
You can enter as many phone numbers as you want. The number-of-digits restriction is separate from the phone numbers allowed restriction. For example, you can choose to allow both. The user may dial a three-digit number or select a specified phone number.

To remove a phone number

Select the phone number and choose Remove.

Stages for Setting up Power-on Password

After an administrator configures the power-on password for a device, the following interactions take place between the user and administrator.

Stage	Who or What	Action
1	Administrator	Configures the power-on password for the user's device.
2	User	Synchronizes the device.
3	User's Device	Prompts the user for a password, stating that the current password must be verified before it can be changed.
4	User	Enters the new password and chooses OK. The password text display is encrypted and cannot be read.
5	User's Device	Prompts the user to enter a password and explains that the password will be required to access the device when it has been locked, turned off, or goes to sleep. Any requirements for the password are also displayed, such as "Must be exactly 4 characters long" and "May only contain: Numerals." The appearance of the screen depends on the password type configured.
6	User	Enters a new password and chooses OK. The password text appears on the screen as the user types it; the text is not encrypted.
7	User's Device (Palm Only)	The Confirm Password screen appears with a message that the password will be required to access the device when it has been locked, turned off, or it goes to sleep.
8	User (Palm Only)	Enters the same password again and presses OK.
9	User's Device	Clears the password screen and allows the user to use the device, starting at the main screen.

Stages for Logging in After Device is Idle

After a user's device is idle for the configured amount of time, the following interactions take place between the user and administrator.

Stage	Who or What	Action
1	User's Device	• If the administrator configured the system *not* to allow any outdialing calls to be made on the locked device, go to Stage 5. • If a restricted outdial number *was* configured, the screen varies, depending on whether the administrator configured a phone number digit restriction and/or a specific phone number restriction.
2	User	Enters or selects the appropriate number. Note: If a restricted number of digits is allowed, the user enters the phone number up to the correct number of digits and chooses Dial. The field will not allow more than the restricted number of digits.
3	User's Device	Calls the appropriate number, using the normal phone mode.
4	User	User completes and terminates the call.
5	User's Device	A screen appears, prompting the user to enter a password. If a restricted outdial number was configured, provides a button to make an outgoing call.
6	User	Does one of the following: • Chooses Call to place a call and returns to Stage 1. • Enters the power-on password to proceed and chooses OK. Continue to stage 7. Note: The password display is encrypted on the device and is case sensitive.
7	User's Device	• If the user enters the correct password, the device - Clears the password screen - Allows the user to use the device • If the user enters an incorrect password, - The user cannot exit the screen until the correct password is entered. • If the user exceeds the maximum number of incorrect attempts - (depends on how the administrator configured it. For more information, see "Configuring Configuration Policy Settings" on page 129).

Stages for Regenerating a Forgotten Password

This section describes the stages that occur when a user forgets their password.

Stage	Who or What	Action
1	Administrator	Optionally configures the system to generate a random password, by following “To generate a random password” on page 88.
2	Device	If the random password feature is configured, sends a new random password back to the server during each Intellisync synchronization. Valid passwords now include either the user-selected password or the new administrator-generated random password. If this is the first time, the user may need to enter an Authentication password first.
3	User	Forgets the password and calls the administrator.
4	Administrator	• If the administrator did not previously set the random password option, instructs the user to hard reset the device. • If the administrator did set the random password feature, looks up the random password and tells the user by doing the following: - On the console, selects Management > Devices > Sync Devices. - Right clicks on a device name and chooses Show Forgotten Password. - Receives a prompt with the generated password. Note: The administrator may have to wait a few minutes after the synchronization to access this information. • Optionally, makes any changes to the Power-on Password settings.
5	User’s Device	• If the administrator configured the system *not* to allow any outgoing calls to be made on the locked device, go to Stage stage 9. • If a restricted outdial number *was* configured, the screen varies, depending on whether the administrator configured a phone number digit restriction and/or a specific phone number restriction.
6	User	Enters or selects the appropriate number. Note: If a restricted number of digits is allowed, the user enters the phone number up to the correct number of digits and chooses Dial. The field will not allow more than the restricted number of digits.
7	User’s Device	Calls the appropriate number, using the normal phone mode.
8	User	User completes and terminates the call.
9	User	Enters the new password, and chooses OK.
10	Device	• If the user enters the correct password, the device - Clears the password screen - Allows the user to use the device - During the next synchronization, generates a new random password (if configured) and sends it back to the server. • If the user enters an incorrect password, - The user cannot exit the screen until the correct password is entered. - If the user exceeds the maximum number of incorrect attempts, (depends on how the administrator configured it. For more information, see “Configuring Configuration Policy Settings” on page 129).

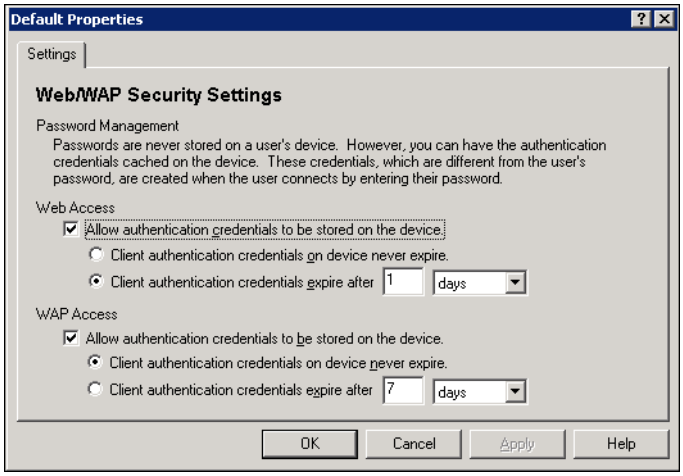
Configuring Web/WAP Security Settings

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

To configure Web/WAP Security settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > General > Web/WAP Security.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The Web/WAP Security Settings Properties dialog box appears.



5. Enter information for the following fields and click OK. You can set these values separately for Web and WAP access.

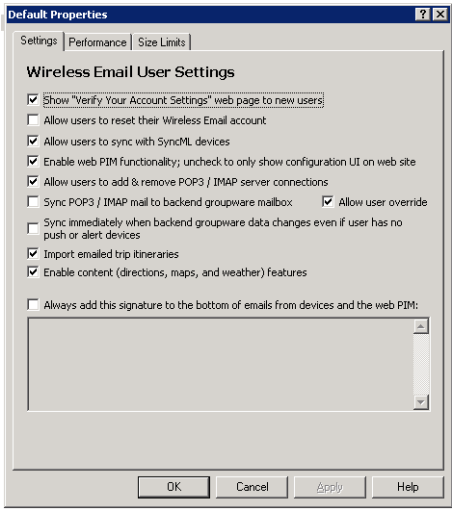
Field	Description
Allow Authentication Credentials To Be Stored On The Device	Select or clear the check box to enable or disable this feature.
Client Authentication Credentials On The Device Never Expire	This option is available only if you select the above option. Select this option to store authentication credentials on user devices indefinitely.
Client Authentication Credentials Expire After <x> <days, minutes, or hours>	This option is available only 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.

Wireless Email Settings

Wireless Email controls are included in the Intellisync Mobile Suite control if you have Wireless Email installed on your server. Wireless Email User profile settings allow you to set user options and permissions.

To configure Wireless Email User settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Wireless Email User.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties. The Wireless Email User Settings Properties dialog box appears with the Settings panel open.



5. Enter information for the following fields and click OK.

Field	Description
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 email 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 clear this option, users can use the Web site only to set up devices.

Field	Description
Allow Users To Add And Remove POP3/IMAP Server Connections	Grants users permission to add connections for POP3 and IMAP map without an administrator's assistance.
Sync POP3/IMAP Mail To Backend Groupware Mailbox	Allows users to synchronize mail from other sources with their corporate Exchange, Domino, or GroupWise account.
Allow User Override	Gives users permission to override the values you select.
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 Nokia Intellisync Mobile Suite server for users who do not have push or alert devices. Setting this option allows for immediate import of emailed itineraries. Nokia recommends that you leave this option cleared for optimum system performance.
Import emailed Trip Itineraries	Enables the feature that recognizes a trip itinerary when it arrives through email, and then automatically imports the trip information into the user's schedule.
Enable Content (Directions, Maps, And Weather) Features	Enables "premium content," including directions, maps, and weather for the user. Premium content is purchased separately and may not be available for all installations.
Always Add This Signature To The Bottom Of emails From Devices And The Web PIM	Add signature information such as name, title, business name and information to appear at the end of every email from a user's device and the web PIM.

To configure User Performance settings

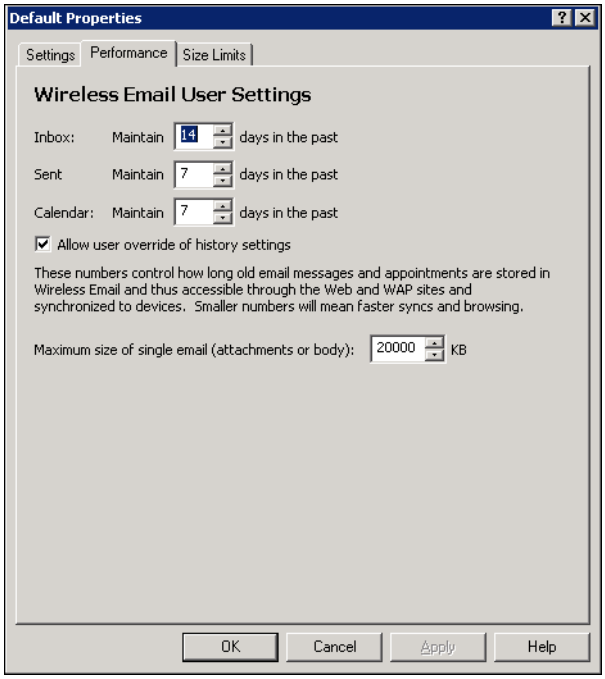
With Wireless Email User Settings, you can control how long items should remain in a user's Inbox, Sent Items, and Calendar folders. In addition, you can control whether users can override these settings.

Note
Less data stored makes device synchronization and browsing faster.

1. Access Wireless Email User Settings properties.

   For more information, see "To configure Wireless Email User settings" on page 93.

2. Choose the Performance tab.



3. Enter information for the following fields and click OK.

Field	Description
Inbox: Maintain <x> Days In The Past	Select the number of days items should remain in the user's Inbox.
Sent: Maintain <x> Days In The Past	Select the number of days items should remain in the user's Sent Items folder.
Calendar: Maintain <x> Days In The Past	Select 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 (Attachments Or Body): <x> kb	Select the maximum number of kilobytes to allow the device to accept for emails or email attachments.

Configuring Wireless Email User Size Limits

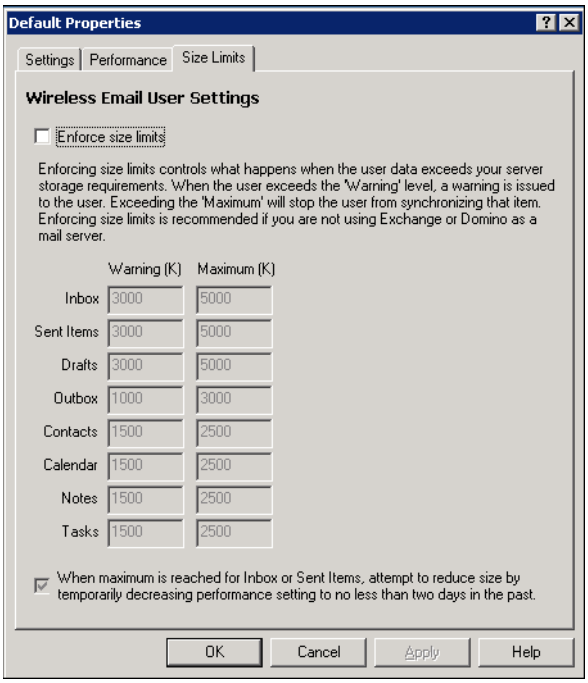
Use the Size Limits panel to control what happens when a user's data exceeds the server storage limits.

To configure User Size Limits settings

1. Access Wireless Email User Settings properties.

   For more information, see "To configure Wireless Email User settings" on page 93.

2. Choose the Size Limits tab.



3. Enter information for the following fields and click OK.

Setting	Description
Enforce Size Limits	Select this option to enable the size limits feature. If you clear this option, other settings on this page become unavailable.
Warning	Set a warning limit for each category. When the user's data exceeds the value, the user receives a warning message.

Setting	Description
Maximum	Set a maximum limit for each category. When the user's data exceeds the value, the user cannot synchronize the current item. **Note** If a user cannot receive or send email, the following message appears: "Message Subject: Undeliverable: <Original Message Subject> Your message did not reach any of the intended recipients because it could not be placed into the Outbox, most likely because your mailbox is full." To resume email activity, the user must delete messages in the Inbox and Sent folders.
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.

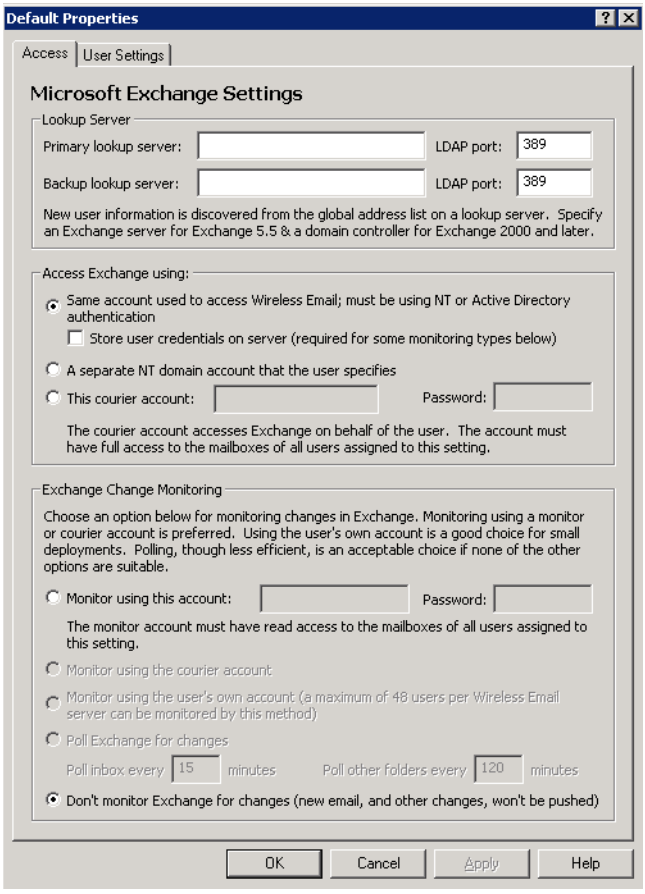
Configuring Microsoft Exchange Settings

Microsoft Exchange profile settings allow you to set values for lookup servers, access methods, user options, and global address list synchronization sessions. For more detailed information about selecting access methods, see Chapter 7, "Authenticating Users."

To configure Microsoft Exchange settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Microsoft Exchange.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

The Microsoft Exchange Settings Properties dialog box appears with the Access panel open.



5. Enter information for the following fields and click OK.

Field	Description
Lookup Server	
Primary Lookup Exchange Server; LDAP Port	Define the name and LDAP port number of the primary lookup server for Microsoft Exchange.
Backup Lookup Exchange Server; LDAP Port	Define the backup lookup server and LDAP port number.
Access Exchange	
Same Account Used To Access Wireless Email; Must Be Using NT Or Active Directory Authentication	Select this option if you want users to connect to the Exchange server using the same Windows NT domain account for accessing Wireless Email.
Store User Credentials On Server; Required For Some Monitoring Types Below	Select this option to implement Push and to perform Contact Lookup on the device.
A Separate NT Domain Account That The User Specifies	Select this option if you want users to connect to the Exchange server using a different Windows NT domain account.
This Courier Account	If users are using a courier account to access the Exchange server, the courier account must have full access to Exchange data for all users employing it. You can create an account with limited privileges for this, or the account can be an existing Exchange “service level administrator” account. • Password—You must provide the password for the courier account. • Confirm Password—Reenter the password for the courier account.
Note: You must store Exchange credentials on the server.	
Exchange Change Monitoring	
Monitor Using This Account	You can use a separate account to monitor changes on the Exchange server. This account must have read rights to the mailboxes of all users assigned to this profile.
Password	Provide the password for this account.
Monitor Using The Courier Account	You can use the courier account to monitor changes on the Exchange server.
Monitor Using The User's Own Account	This method is limited to a maximum of 48 users per server.

Field	Description
Poll Exchange For Changes	You can specify a time interval, in minutes, for the Inbox and other folders in the database to be checked for changes.
Don't Monitor Exchange For Changes	The database is not checked for changes.

Configuring Microsoft Exchange User Settings

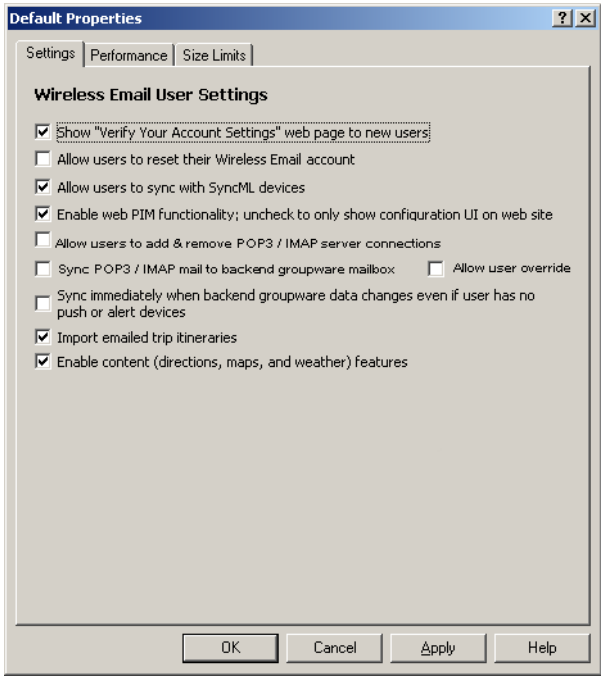
The User Settings panel has settings for user options and global address list synchronization. You can have users synchronize the entire global address list, a portion of the global address list, or none of it.

To configure Microsoft Exchange settings

1. Access Microsoft Exchange Settings properties.

   For more information, see "To configure Microsoft Exchange settings" on page 97.

2. Choose the User Settings tab.

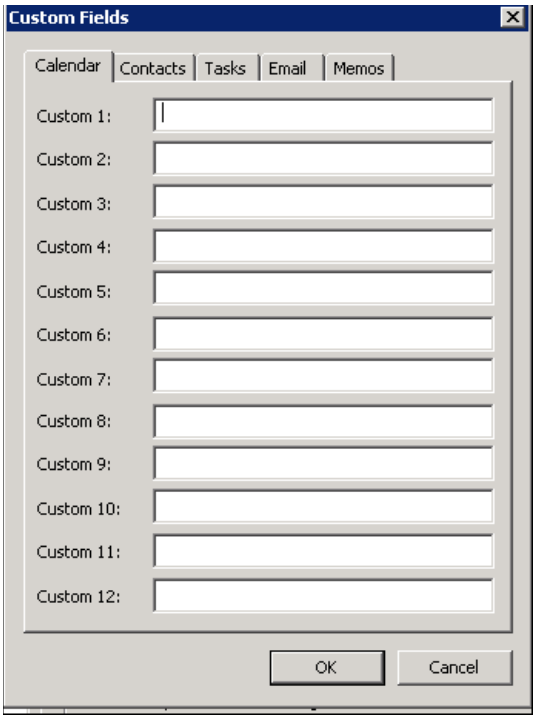


3. Enter information for the following fields and click OK.

Field	Description
User Options and Capabilities	
Show Exchange UI On The Registration Web Page And Discover User's Mailbox If Possible	Select this option if you want the user to view Microsoft Exchange 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 To Not Connect To Exchange	Select this option to give users the choice of having a handheld device that uses Microsoft Exchange as the messaging platform.
Allow Users To Manually Add / Remove Exchange Server Connections	Controls whether users can add or remove handheld devices that are using Microsoft Exchange as their messaging platform.
Delete Items Permanently; Don't Move Them To Deleted Items	This option allows items to be removed immediately and permanently rather than moving them to Deleted Items where they could be restored.
Global Address List Synchronization Settings	
Don't Sync Global Address List	Select this option so the global address list does not synchronize.
Sync The Members Of These Distribution Lists	Select specific groups, if any, you want to synchronize.
Sync Entire Global Address List	Select this option to synchronize the entire global address list.
Allow User Override Of Global Address List Sync Settings	Select this option to allow the user to override the global address list synchronization features you define here.

To define custom fields

1. On the User Settings panel, choose Custom Fields.



   Choose the tab for which you want to create custom fields.

2. Enter the information in the appropriate field, and choose OK.

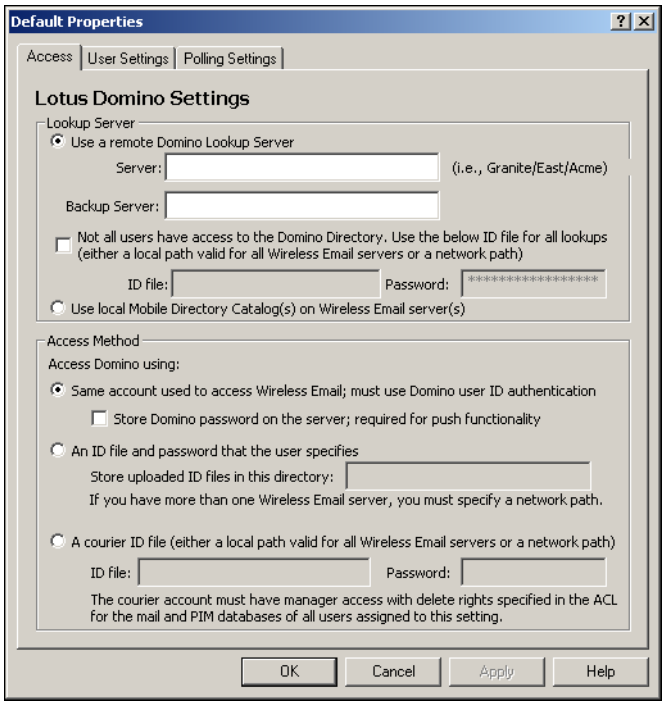
Configuring Lotus Domino Settings

Lotus Domino profile settings allow you to set values for lookup servers, access methods, user options, personal address books, journals, and shared contacts. For more information about selecting access methods, see Chapter 7, “Authenticating Users.”

To configure Domino settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Lotus Domino.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

The Domino Settings Properties dialog box appears with the Access panel open.



5. Complete the fields to enter a lookup server and then select an access method for the user.

Field	Description
Lookup Server	
Use A Remote Domino Lookup Server	Select this option and specify a lookup server in the next field.
Server	Type the name of the Domino Lookup Server.
Backup Server	Type the name of the Domino Lookup Backup Server.
Not All Users Have Access To The Domino Directory	Select this option if some users do not have access to the Domino directory. Then, provide the ID file for all lookups (either a local path valid for all Wireless Email servers or a network path). • ID file—Unless all users have access to the Domino directory, specify an ID file to use for lookups. Use either a local path valid for all Wireless Email servers or a network path. • Password—Type the password for the Domino Lookup server.
Use Local Mobile Directory Catalog(s) On Wireless Email Server(s)	Select this option to resolve email addresses using local Mobile Directory Catalogs instead of a lookup server.

Field	Description
Access Method	
Same Account Used To Access Wireless Email; Must Be Using Domino User ID Authentication	Select this option if you want users to connect to the Domino server using the same account users use to access Wireless Email. Use Domino User ID authentication to decrypt mail for viewing on a device. Store Domino Password on the Server; Required for Push Functionality—Select this option if you want to send data to users without the users requesting it.
An ID File And Password That The User Specifies	Select this option if the user can specify a logon account. Enter the name of the directory on the Wireless Email server in which to store the uploaded ID files. If more than one Wireless Email server exists, specify a network path. Store Uploaded ID Files in this Directory—Use this field to specify the directory where you want to store uploaded ID files. If you are using clustered Wireless Email servers, you must specify a network path.
A Courier ID File	If you are using a courier account, you can specify either a local path valid for all Wireless Email servers or a network path. The account must have manager access with delete permissions specified in the ACL for the email and PIM databases of all users assigned to this setting. • ID file—Specify the name (and network path if required) of the ID file. • Password—Type the password for the courier account.

Configuring Domino User Settings

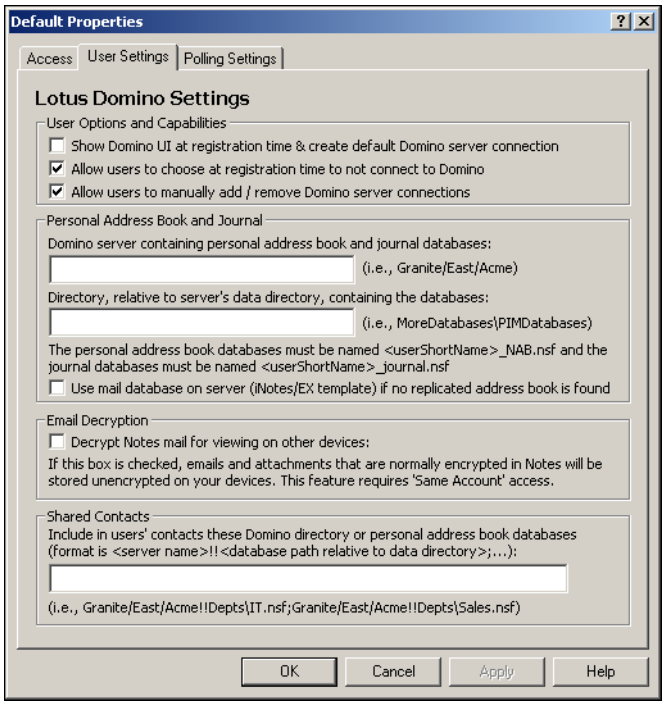
The Lotus Domino User Settings profile settings allow you to configure user options, personal address book and journal, and shared contacts.

To configure Domino User settings

1. Access Lotus Domino Settings properties.

   For more information, see "To configure Domino settings" on page 102.

2. Choose the User Settings tab.



3. Enter information for the following fields and click OK.

Field	Description
User Options and Capabilities	
Show Domino UI At Registration Time And Create Default Domino Server Connection	Select this option if you want the user to view the Domino user interface when registering on the Web. If you select this option, the system creates a default server connection.
Allow Users To Choose At Registration Time Not To Connect To Domino	Select this option if you do not want the user to designate a server when registering.
Allow Users To Manually Add / Remove Domino Server Connections	Select this option to allow users to add or remove server connections.
Personal Address Book And Journal	
Domino Server Containing Personal Address Book And Journal Databases	List the Domino server containing the databases you want to access. (Leave blank to look only on the root directory of user's mail server.)
Directory, Relative To Server's Data Directory, Containing The Databases	Enter the directory that contains the databases. (Leave blank to look only on the root directory of user's mail server.)

Field	Description
Use Mail Database On Server If No Replicated Address Book Is Found	Select this option so that the system defaults to the mail database on the server if no other address book is found.
email Decryption	
Decrypt Notes Mail For Viewing On Other Devices	Select this option if you want to store email messages and attachments as unencrypted on the device. (This option requires Same Account access.)
Shared Contacts	
Include In Users' Contacts These Domino Directory Or Personal Address Book Databases	Select this option to list the databases you want the user to access for contacts

Configuring Domino Polling Settings

Domino Polling profile settings allow the server to open your users' Notes databases at regular intervals and checks for changes. If Nokia Intellisync Mobile Suite find changes, it synchronizes and pushes the data to the appropriate devices.

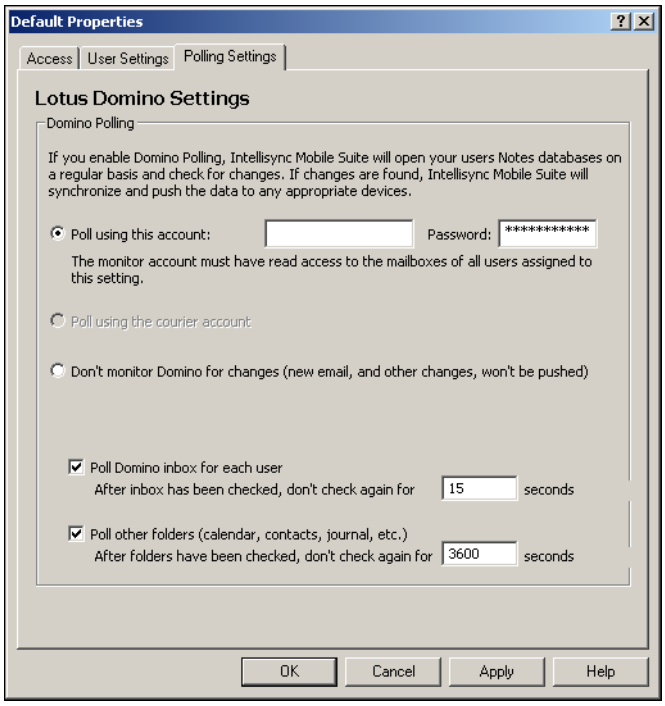
To configure Domino Polling settings

Domino Polling allows you to synchronize and push Lotus Notes inbox, calendar, task, contact, and journal items to the appropriate devices at regular intervals.

1. Access Lotus Domino Settings properties.

   For more information, see "To configure Domino settings" on page 102.

2. Choose the Polling Settings tab.



3. Enter information for the following fields and click OK.

Field	Description
Poll Using This Account	User ID and password of the account assigned for polling.
Poll Using The Courier Account	Select this option if polling is set for a courier account.
Don't Monitor Domino For Changes	Select this option if you do not want new email and other changes to be pushed.
Poll Domino Inbox, For Each User. After Folders Have Been Checked	Place a check mark in the box if you want to poll the inbox for each Notes user. Don't Check Again for <x> Minutes—Type the number of minutes you want to wait before checking the Notes database again.
Poll Other Folders	Place a check mark in the box if you want to poll for calendar events, contacts, and journal items for each Notes user. Don't Check Again for <x> Minutes—Type the number of minutes you want to wait before checking the Notes database again.

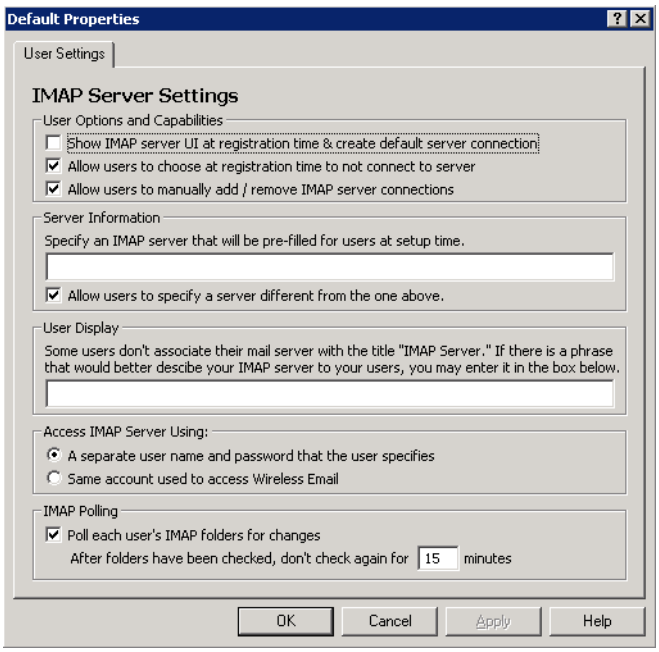
Configuring IMAP Server Settings

IMAP Server profile settings allow you to configure and modify IMAP server settings.

To configure IMAP Server settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > IMAP Server.
3. In the details pane, select the profile you want to view and choose Action > Properties.

   The IMAP Server Settings Properties dialog box appears.



4. Enter information for the following fields and click OK.

Field	Description
User Options And Capabilities	Select an option for server connection. • Show IMAP server UI at registration time and create default server connection. • Allow users to choose at registration time to not connect to the server. • Allow users to manually add or remove IMAP server connections.
Server Information	• Specify the default IMAP server. • Select if users can specify an IMAP server other than the default.
User Display	Type a descriptive name or phrase for your IMAP server. This field is optional.

Field	Description
Access IMAP Server Using	Select this option to access the IMAP server using a different user name and password or the same user name and password used to access Wireless Email.
IMAP Polling	Select this option to enable IMAP IDLE change monitoring and polling. If enabled, Nokia Intellisync Mobile Suite attempts an IMAP IDLE connection with the IMAP server at specified time intervals, and uses polling only if IMAP IDLE is not available.

Configuring LDAP GAL Lookup Settings

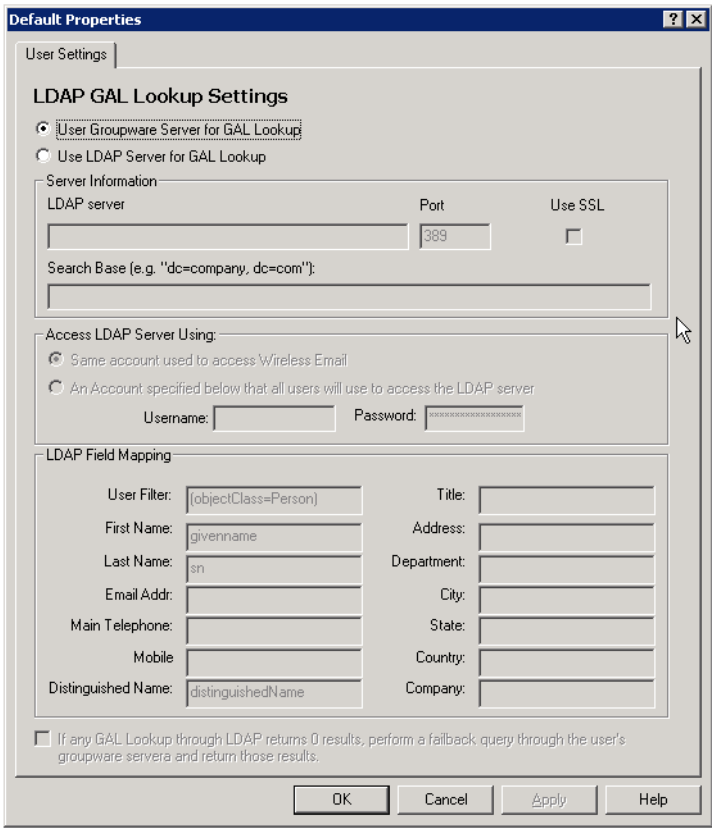
Global address list (GAL) lookups provide users the ability to look up corporate employee contact information from a mobile device.

LDAP GAL Lookup profile settings allow you to configure GAL against an LDAP (Lightweight Directory Access Protocol) source or other groupware, such as Microsoft Exchange, Lotus Domino, or Novell GroupWise.

To configure LDAP GAL Lookup settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > LDAP GAL Lookup.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

The LDAP GAL Lookup Settings Properties dialog box appears.



5. Enter information for the following fields click OK.

Field	Description
Use Groupware Server For GAL Lookup	Select this option to configure GAL lookups against groupware systems such as Microsoft Exchange, Lotus Domino, or Novell GroupWise.
Use LDAP Server For GAL Lookup	Select this option to configure GAL lookups against the corporate LDAP server, such as a Microsoft active directory server.
Server Information	
LDAP Server	The fully qualified name or IP address for the corporate LDAP server to which Nokia Intellisync Mobile Suite can connect.
Port	LDAP server socked port that receives incoming connections and requests.

Field		Description
Use SSL		Use a Secure Sockets Layer (SSL) connection to the LDAP server.
Search Base		The root node distinguished name (DN) on which the corporate LDAP server bases its searches.
Access LDAP Server Using		
Same Account Used To Access Wireless Email		Select this option to configure the corporate LDAP server to accept the same logon credentials for Wireless Email.
An Account Specified Below That All Users Will Use To Access The LDAP Server		Select this option to configure the corporate LDAP server to accept a general user name and password logon for all users to connect to the LDAP server. Username—User ID to access the LDAP server Password—Password to access the LDAP server
LDAP Field Mapping	**Required/Optional**	
User Filter	Required	User filter field name defined in the LDAP server For example: (objectClass[Person])
First Name	Required	User first name field defined in the LDAP server. For example: givenname
Last Name	Required	User last name field defined in the LDAP server. For example: sn
email Address	Optional	User email address field defined in the LDAP server.
Main Telephone	Optional	User main telephone field defined in the LDAP server.
Mobile	Optional	User cell phone number field defined in the LDAP server.
Distinguished Name	Required	User distinguished name field defined in the LDAP server. For example: distinguishedName
Title	Optional	User title field defined in the LDAP server.
Address	Optional	User address field defined in the LDAP server.
Department	Optional	User department field defined in the LDAP server.
City	Optional	User city field defined in the LDAP server.
State	Optional	User state field defined in the LDAP server.
County	Optional	User county field defined in the LDAP server.
Company	Optional	User company field defined in the LDAP server.

Field	Description
If Any GAL Lookup Through LDAP Returns 0 Results, Perform A Failback Query Through The User's Groupware Servers And Return Those Results	Initiate a failback query that rechecks the corporate LDAP server for valid results and performs a lookup against any other groupware systems (such as Microsoft Exchange, Novell GroupWise, or Lotus Domino).

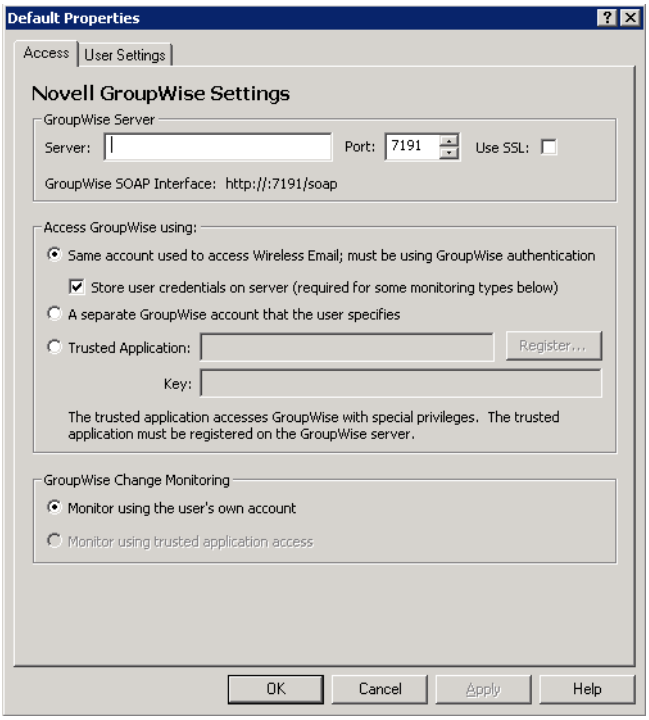
Configuring Novell GroupWise Settings

Novell GroupWise profile settings allow you to set values for the server, access methods, user options, and system address book synchronization sessions. For more information about selecting access methods, see Chapter 7, "Authenticating Users."

To configure Novell GroupWise access settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Novell GroupWise.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The Novell GroupWise Settings Properties dialog box appears with the Access panel open.



Field	Description
GroupWise Server	
Server	Enter the name of the GroupWise server.
Port / SSL	Define the name, port number and SSL state of the GroupWise server that runs the SOAP listener.
Access GroupWise	
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 for accessing Wireless Email.
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. For more information, refer to the next section, "Creating a Trusted Application With GroupWise" on page 113.
Key	If a trusted application is used, enter the application key for the registered trusted application.
GroupWise Change Monitoring	
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 then assigned to GroupWise Mobile Server for accessing GroupWise.

If you use a trusted application, 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"

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

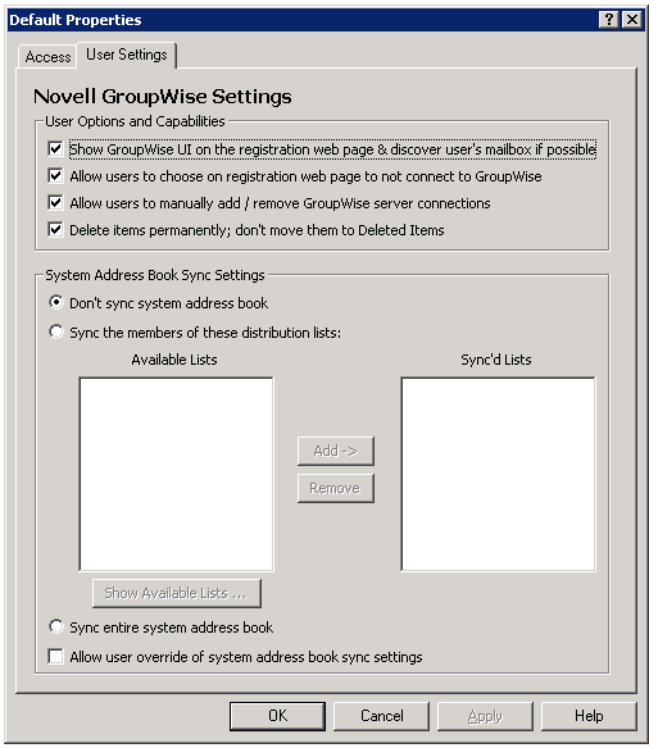
Configuring Novell GroupWise User Settings

Novell GroupWise User profile settings allow you to configure user options and system address book synchronization.

To configure Novell GroupWise settings

1. Access Novell GroupWise Settings properties.

   For more information, see “To configure Novell GroupWise access settings” on page 112.
2. Choose the User Settings tab.



3. Enter information for the following fields and click OK.

Field	Description
User Options and Capabilities	
Show GroupWise UI On The Registration Web Page And 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.
Delete Items Permanently; Don't Move Them To Deleted Items	Select this option to delete the items permanently.
System Address Book Sync Settings	
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, if any, you want to synchronize.
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.

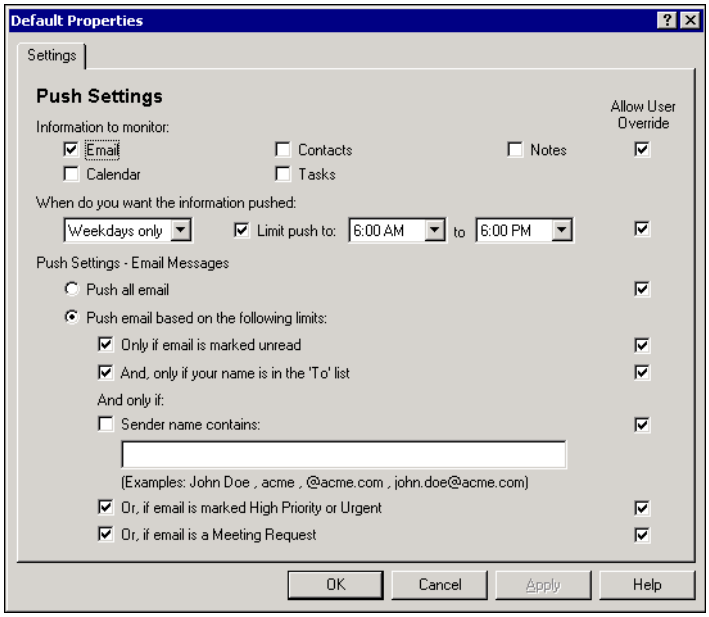
Configuring Push Settings

Push profile settings allow you to configure Push values.

To configure Push settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Push.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

5. The Push Settings Properties dialog box appears.



6. Enter information for the following fields and click OK.

Field	Description
General	
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 everyday or only on weekdays.
Limit Push To <starttime> To <stoptime>	Use the list to select the time range in which users are to receive pushes.
Push Settings - email Messages	
Push All email	Select this option to have all email messages pushed, regardless of any factors

Field	Description
Push Email Based On The Following Limits	By selecting from the following criteria, you can set limits on the types of email messages you want to receive: • Only if email is marked unread • And, only if your name is in the To list • Sender name contains <text> • Or, if email is marked High Priority or Urgent • Or, if email is a Meeting Request

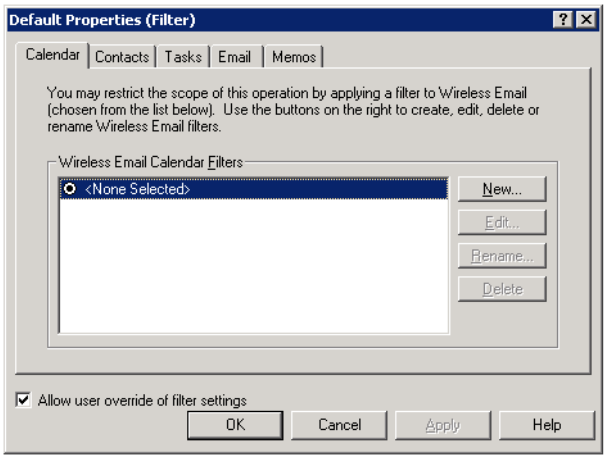
Configuring Filter Settings

Filter profile settings allow you to define LDAP search filters for PIM information.

To configure Filter settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Filter.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The Filter Properties dialog box appears with the Calendar panel open.

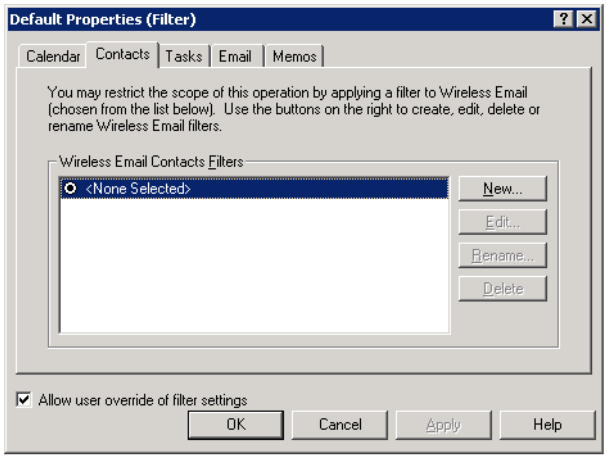


To configure the Contacts Filter

1. Access Filter properties.

   For more information, see "To configure Filter settings" on page 117.

2. Choose the Contacts tab.



To configure the Tasks Filter

1. Access Filter properties.

   For more information, see "To configure Filter settings" on page 117.

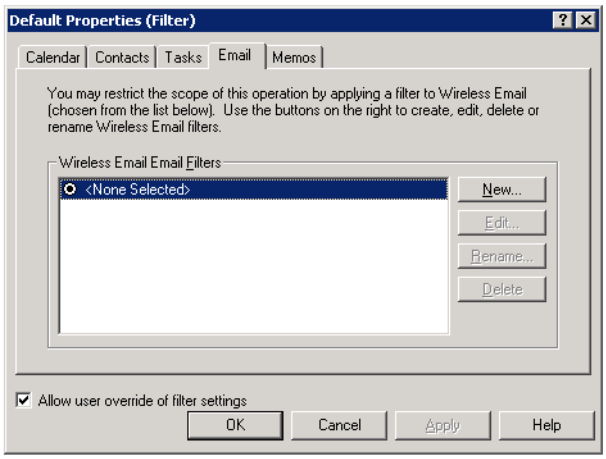
2. Choose the Tasks tab.

To configure the Email Filter

1. Access Filter properties.

   For more information, see "To configure Filter settings" on page 117.

2. Choose the Email tab.

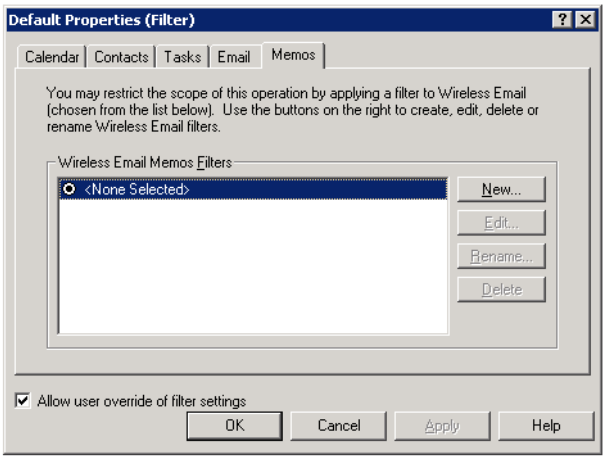


To configure the Memos Filter

1. Access Filter properties.

   For more information, see “To configure Filter settings” on page 117.

2. Choose the Memos tab.



Sync and SyncXpress

For many of the settings screens, two panels exist: the Sync panel and the SyncXpress panel. 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. A Copy To button on the panel copies information between the two panels.

Sync and SyncXpress settings are available for the following sections:

- “Configuring Inbox and Outbox Settings” on page 119
- “Configuring Sent Items Settings” on page 121
- “Configuring Drafts Settings” on page 122
- “Configuring PIM Settings” on page 124

Configuring Inbox and Outbox Settings

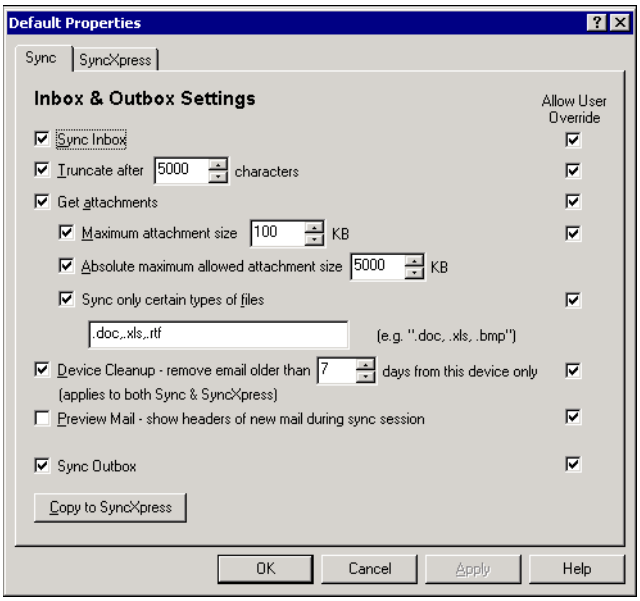
Inbox and Outbox profile settings allow you to set combinations of values for message truncation, attachment limitations, old mail deletion, and preview.

To configure Inbox and Outbox settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Inbox and Outbox.

3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The Inbox And Outbox Settings Properties dialog box appears with the Sync panel open.



5. Enter information for the following fields and click OK.

Field	Description
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 email. • Maximum attachment size (in KB)—Specify a size limit (in kilobytes) for the attachments to conserve space and minimize download times. • 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 will not download if it exceeds the value you set here. • Sync Only Certain Types of Files—Synchronize only attachments of a certain file type (such as .doc, .xls, and so forth).
Device Cleanup – Remove email Older Than <x> Days From This Device Only	(Applies to both Sync And SyncXpress) Enter the number of days to keep email on the user's device.

Field	Description
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 email 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 panel and want to apply the same settings to the SyncXpress panel, choose Copy To SyncXpress. If you set values on the SyncXpress panel and want to apply the same settings to the Sync panel, choose Copy To Sync.
Allow User Override	For each option on this page, you can control whether users can override the values you set.

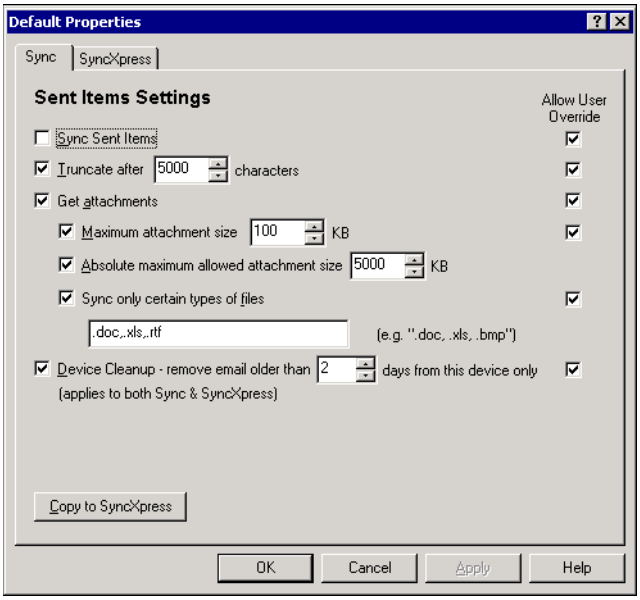
Configuring Sent Items Settings

Sent Items profile settings allow you to set up truncation, attachment options, and email deletion.

To configure Sent settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > Sent Items.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The Sent Items Settings Properties dialog box appears with the Sync panel open.



5. Enter information for the following fields and click OK.

Field	Description
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 email. • Maximum Attachment Size (in KB)—Specify a size limit (in kilobytes) for the attachments to conserve space and minimize download times. • 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 will not be 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 email Older Than <x> Days From This Device Only	(Applies to Both Sync And SyncXpress) Enter the number of days to keep sent email on the user's device.
Copy To SyncXpress / Copy To Sync	If you set values on the Sync panel and want to apply the same settings to the SyncXpress panel, choose Copy To SyncXpress. If you set values on the SyncXpress panel and want to apply the same settings to the Sync panel, choose Copy To Sync.

Configuring Drafts Settings

Profile settings for draft messages are similar to the Inbox and Sent Items settings and include truncation and attachment options.

To configure Drafts settings

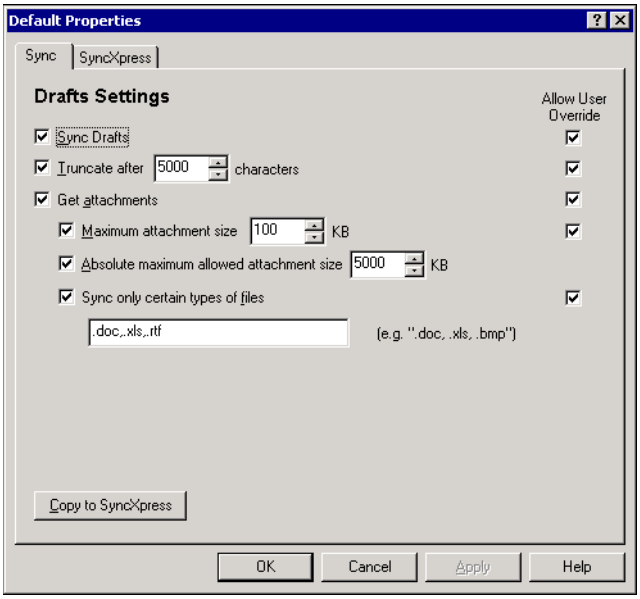
1. From the console tree, select Intellisync Mobile Suite.

2. Expand Profile Settings > Wireless Email > Drafts.

3. In the details pane, select the profile you want to view.

4. Choose Action > Properties.

The Drafts Settings Properties dialog box appears with the Sync panel open.



5. Enter information for the following fields and click OK.

Field	Description
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 sent message.
Get Attachments	Select this option to allow the device to receive file attachments in email. • Maximum Attachment Size (in KB)—Specify a size limit (in kilobytes) for the attachments to conserve space and minimize download times. • 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 will not be 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 panel and want to apply the same settings to the SyncXpress panel, choose Copy To SyncXpress. If you set values on the SyncXpress panel and want to apply the same settings to the Sync panel, choose Copy To Sync.

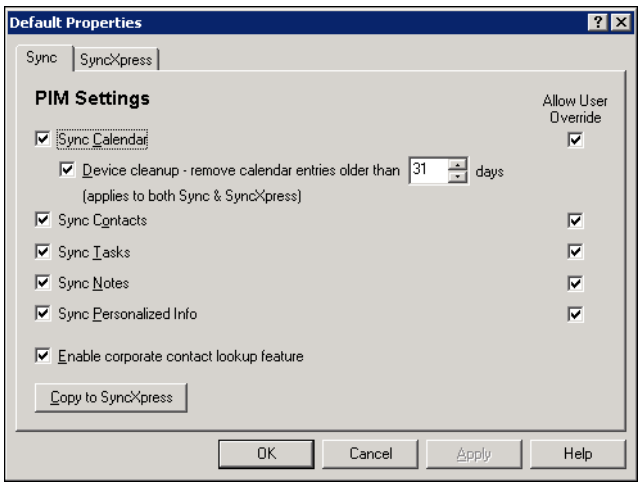
Configuring PIM Settings

PIM profile settings allow you to configure Calendar, Contacts, Tasks, Notes, and Personalized Information options.

To configure PIM settings

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Wireless Email > PIM.
3. In the details pane, select the profile you want to view.
4. Choose Action > Properties.

   The PIM Settings Properties dialog box appears with the Sync panel open.



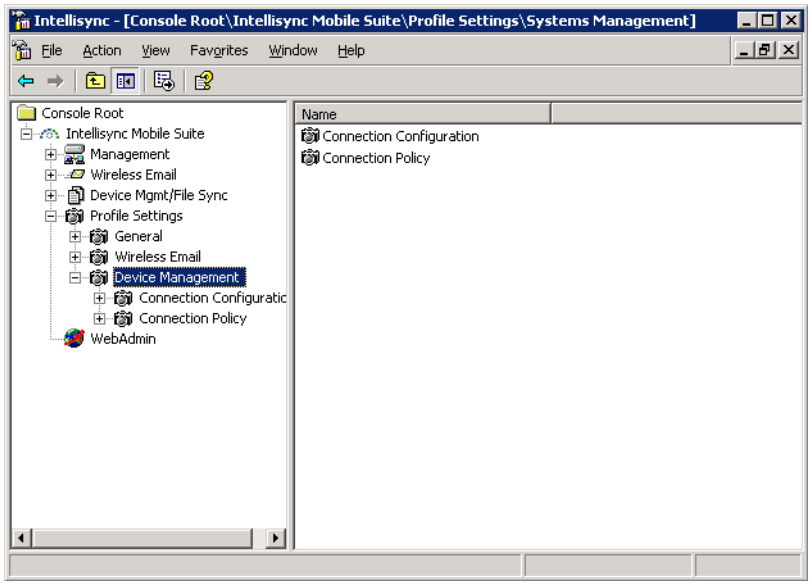
5. Enter information for the following fields and click OK.

Field	Description
Sync Calendar	Select this option to synchronize users' Calendar information.
Device Cleanup – Remove Calendar Entries Older Than <x> Days	(Applies to Both Sync And SyncXpress) Enter 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.

Field	Description
Enable Corporate Contact Lookup Feature	The corporate contact lookup feature may 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 panel and want to apply the same settings to the SyncXpress panel, choose Copy To SyncXpress. If you set values on the SyncXpress panel and want to apply the same settings to the Sync panel, choose Copy To Sync.

Device Management Settings

The Device Management control appears in the Nokia Intellisync Mobile Suite control if you have Device Management installed on your server.



Configuring Connection Configuration Settings

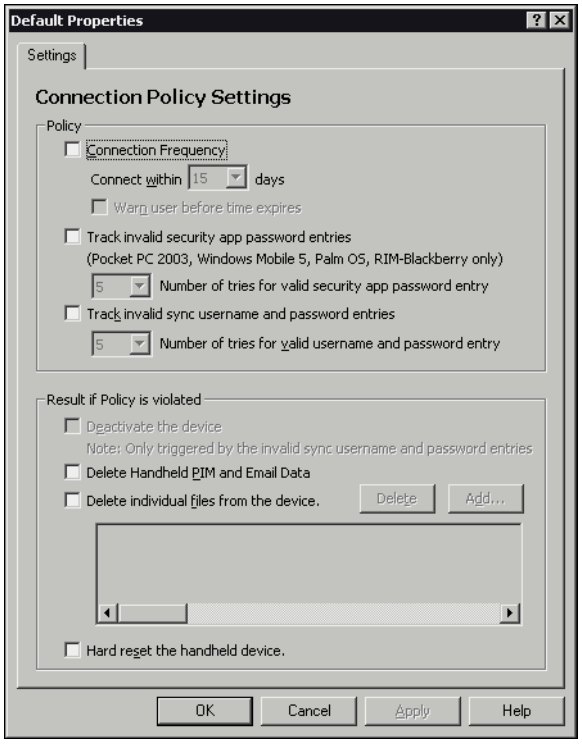
Connection Configuration profile settings allow you to set up your connection to communicate with the server. Specify the options to use for the connection.

In addition to a network connection, if available, select from any modem connection you have. Choose the connection to use as the default or choose a different connection for a specific session.

To configure the connection

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Device Management > Connection Configuration.
3. In the details pane, select the connection configuration you want to view.
4. Choose Action > Properties.

   The Connection Configuration Settings Properties dialog box appears.



To add a Windows Mobile connection

1. On the Connection Configuration Settings screen, select one of the following connection types:
   - PC Connection (only supported for Windows 2000 / XP clients)
   - Pocket PC / Win CE Connections
   - Smartphone Connections
2. Choose Add Connection.

   The Add connection dialog box appears.
3. Enter the name for the connection configuration, and choose OK.

To add a Palm connection

1. On the Connection Configuration Settings screen, select Palm OS Connections.

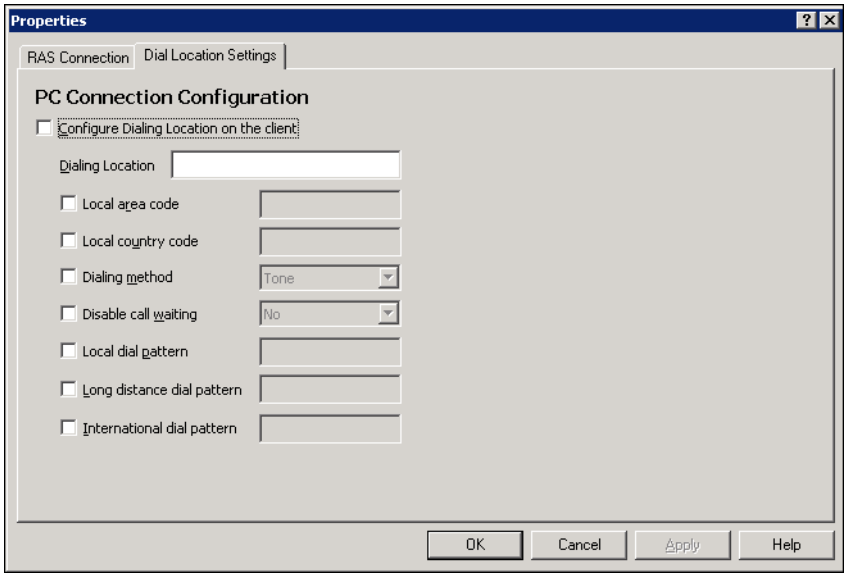
   The PC Connection Configuration Properties screen appears with the RAS Connection panel open.

2. Enter information for the following fields and click OK.

Field	Description
Configure RAS Settings On The Client	
General	
RAS Name	Enter the name for the RAS settings, and select the appropriate action to add, modify, or remove the setting.
Set As Default Connection On Device	Use the connection as the default for the device.
Username	Enter the user name for the device.
Require User To Re-enter Password On Next Connection	Add security by forcing the user to enter a password each time a connection occurs.
Area Code	Check this option and enter the area code to set as the default for the connection.
Phone #	Check this option and enter the phone number to set as the default for the connection.
IP Settings for RAS Connection	
Obtain An IP Address Automatically	• Check this option and select Yes to have the server obtain an IP address automatically for the RAS connection • Check this option and select No to select *not* to have the server obtain an IP address automatically for the RAS connection. • Specific IP Addr—Always connect to a specific IP address, and enter the IP address.
Obtain DNS Server Address Automatically	• Check this option and select Yes to have the server obtain a DNS server address automatically for the RAS connection. • Check this option and select No to select *not* to have the server obtain a DNS server address automatically for the RAS connection. • Primary DNS—Specify the primary DNS server for RAS connection, and enter the IP address. • Alternate DNS—Specify an alternate DNS server for RAS connection, and enter the IP address. • Primary WINS—Specify the primary WINS server for RAS connection, and enter the IP address. • Alternate WINS—Specify an alternate WINS server for RAS connection, and enter the IP address.

Field	Description
User SLIP	Serial Line Internet Protocol (SLIP) used for sending data across serial lines.
Compression	Compressed Serial Line Internet Protocol (SLIP) used for sending data across serial lines.

3. Choose the Dial Location Settings tab.



4. Enter information for the following fields, and choose OK.

Field	Description
Configure Dialing Location On The Client	Phone number to dial for RAS connection. Dialing Location—Enter the phone number to dial.
Local Area Code	Area code number to dial for RAS connection, and enter it in the text box.
Local Country Code	Local country code number to dial for RAS connection, and enter it in the text box.
Dialing Method	Dialing method to dial for RAS connection, and select it from the list box,
Disable Call Waiting	Disable call waiting, which can interrupt dialing for RAS connection, and select No in the list box.
Local Dial Pattern	Local dial pattern to dial for RAS connection, and enter it in the text box.

Field	Description
Long Distance Dial Pattern	Long distance dial pattern to dial for RAS connection, and enter it in the text box.
International Dial Pattern	International dial pattern to dial for RAS connection, and enter it in the text box.

Configuring Configuration Policy Settings

If a user's device gets lost or stolen, you can protect the data by using the Configuration Policy settings to deactivate the device, delete PIM and email data and individual files, and hard reset the device, which erases all personal data from the device.

You can push any of the following options to a specific device from the administrator console. Additionally, users can log in to their user web site and control their own devices, including device lock, delete PIM and email data, or hard reset the device.

These options can be immediately pushed by the administrator to a specific device from the administration console. Additionally, users can log in to their user web site and control their own devices including device lock, delete PIM and email data, or hard reset the device.

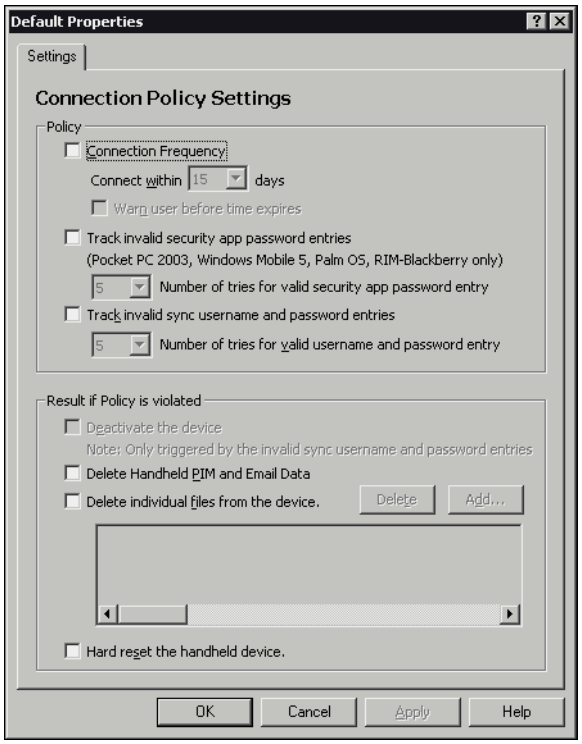
The following table displays the theft/loss protection features to clients:

	Windows Mobile	Symbian	Palm	Blackberry
PIM/email	✓	✓	✓	x
Hard Reset	✓	✓	✓	✓
Device Lock	✓	✓	✓	✓

To configure the connection policy

1. From the console tree, select Intellisync Mobile Suite.
2. Expand Profile Settings > Device Management > Connection Policy.
3. In the details pane, select the connection policy you want to view.
4. Choose Action > Properties.

The Connection Policy Settings Properties dialog box appears.



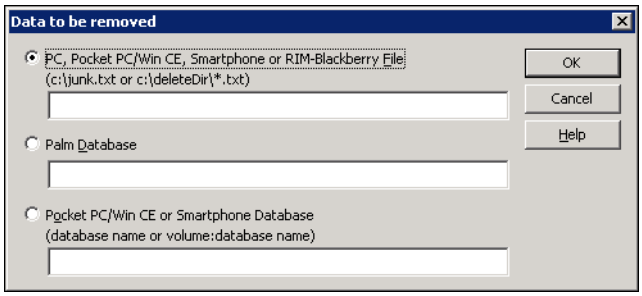
5. Enter information for the following fields and click OK.

Field	Description
Policy	
Connection Frequency	Check this option and select the frequency (in days) with which you want to connect.
Track Invalid Security App Password Entries	Track the number of invalid logon attempts made to a device. Enter the number of valid attempts allowed before the device enforces the connection policy defined in Result if Policy is Violated.
Track Invalid Sync Username and Password Entries	Track the number of invalid synchronization authentication attempts made to a device. Enter the number of valid authentication attempts allowed before the device enforces the connection policy defined in Result if Policy is Violated.
Result If Policy Is Violated	
Deactivate The Device	Deactivate the device if the number of invalid logon or synchronization authentication attempts allowed is exceeded. The user cannot use the phone or other functions or synchronize, and must contact the administrator for help.

Field	Description
Delete Handheld PIM And Email Data	Delete all email and personal information (such as calendar appointments, contacts, tasks, and memo information) from the device if the number of invalid logon or synchronization authentication attempts allowed is exceeded.
Delete Individual Files From The Device	Delete specific directories, sub-directories, or files from the device if the number of invalid logon or synchronization authentication attempts allowed is exceeded. Specify the file names in the text box.
Hard Reset The Handheld Device	Perform a hard reset of the device if the number of invalid logon or synchronization authentication attempts allowed is exceeded. A hard reset returns the device to a new device state removing all personal data, email messages, applications, and files added since first getting the device.

6. To remove data, choose the Add button.

The Data to Be Removed dialog box appears.



7. Enter the information in the dialog box, and choose OK.

Field	Description
PC, Pocket PC/Win CE, Smartphone Or RIM-Blackberry File	Check the box and enter the name of the patch and file name to remove,
Palm Database	Check the box and type the name of the Palm database to remove.
Pocket PC/Win CE Or Smartphone Database	Check the box and enter the name of the Pocket PC, Win CE, or Smartphone database to remove.

Restricting Hardware Elements on a User's Device

You can restrict the use of hardware elements such as sound, speaker, Blue Tooth, camera, WIFI, and other hardware components on specified devices. You select the elements you want to restrict on the predefined list and then assign the list to users or groups.

To access the Hardware Restrictions control

1. From the console tree, expand the Device Management control.
2. Select Hardware Restrictions.
3. Choose a hardware restrictions configuration.
4. Select Action > Properties.

   The Hardware Restriction Settings window appears.
5. Select the hardware elements you want to disable for a particular device. Available options include the following.
   - Camera
   - Global Positioning System (GPS)
   - Bluetooth
   - Infrared
   - Remote Networking
   - Wireless Fidelity (WiFi)
   - Compact Flash
   - Secure Digital (SD) Card
   - Short Message Service (SMS)
   - Sound
   - Speakerphone
6. Click OK.

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 Nokia Intellisync Mobile Suite control, you can:

- Create a profile setting
- Change options and properties for a profile setting
- Apply profiles to users and groups
- Prioritize profile settings
- Delete a profile setting

Creating Profile Settings

Nokia Intellisync Mobile Suite provides default profile settings for each option. These default settings may be sufficient for your company for certain features. You can 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.

To create a profile setting

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. Choose Action > Create New Setting.

   The Create New Setting dialog box appears.
4. In the New Setting Name field, type a name for the setting.
5. From the list, select an existing profile setting where values are similar to the setting you want to create. This decreases the set up time for the new setting. (This step is optional.)
6. Choose OK.

   The Properties dialog box for the new setting appears.
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. Choose OK.

Using Properties to Change Profile Settings

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

To access the Properties dialog box

1. From the console tree, expand Profile Settings.
2. Navigate to the profile setting you want to change.
3. Select the profile.
4. Choose Action > Properties.

   The Properties dialog box appears for the designated profile setting.
5. Complete the changes for the setting.
6. Choose OK.

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 about assigning profile settings to users and groups, see "Assigning/Editing User Profiles" on page 62 and "Assigning/Editing Group Profiles" on page 66.

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. Choose Action > Prioritize Profile Assignments.

   The Prioritize Profile Assignments dialog box appears.
3. In the Profile Priority list, select the group name to which you want to assign the highest priority.
4. Choose 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. Choose OK.

Deleting Profile Settings

You can delete profile settings you no longer need.

To delete a profile setting

1. From the console tree, expand Profile Settings.
2. Navigate to the profile setting you want to delete.
3. Select the profile.
4. Choose Action > Delete.
5. Choose 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 once it is no longer in use.

5 Security

Access to corporate information assets using mobile devices creates a variety of security challenges. Nokia Intellisync Mobile Suite 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.

Intellisync Mobile Suite has a security strategy that addresses the following areas:

- Authentication—Guarantees that users are authorized to connect.
- Access to Specific Information—Managing access and authorization to control the information delivered to users.
- Encrypting 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 Nokia Intellisync Mobile Suite server relative to existing firewalls and allowing it to communicate with other servers.

Authentication

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

The following authentication approaches are available:

- Domain— alidate users through Windows NT Domain Controllers.
- Lotus Domino—Validate users through the Domino server.
- Novell GroupWise—Validate users through the GroupWise server.
- LDAP—Validate users through an LDAP source, such as Active Directory.
- Intellisync—Validate users using a list of users created and maintained through the Intellisync Mobile Suite control.

Your security strategy can incorporate one or more 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 Intellisync's security strategies. For more information on selecting and implementing authentication strategies, refer to Chapter 7, "Authenticating Users."

Domain, Domino, GroupWise, or LDAP Authentication

You may be able to leverage the authentication methods you currently use to avoid duplicate efforts in entering and maintaining user lists. For example, if you use network domain verification, users can log on by using their existing network user names and passwords. This approach to authentication may simplify the maintenance and user's experience.

Changes to the corporate user directory automatically appear in the Admin Console. This feature eliminates any need for duplicate user administration activity. For example, it eliminates the need to remove a former employee from multiple directories.

Intellisync Authentication

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

Even if you select Domain, Domino, or GroupWise, 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.

A combined approach can be useful for testing or for migrating from one authentication approach to another. Nokia Intellisync Mobile Suite authenticates each user with only one method, but you can use any method for a given user.

User Access

For some Nokia Intellisync Mobile Suite products, authentication is all that is required for a user to connect and communicate with the server. For PIM and email synchronization, however, there are two requirements for allowing a user to connect and access email and PIM data:

- Authentication with Nokia Intellisync Mobile Suite server
- Access to the mail server

Chapter 7, "Authenticating Users" contains more information about authenticating users for all products. Chapter 8, "Granting Access to the Mail Server" includes mail server information and applies only to Wireless Email.

Access to Specific Information

After the user passes authentication, the Nokia Intellisync Mobile Suite server determines the information each user can access. For example, access to email and PIM information is set up using profile settings. For more information, see Chapter 4, "Profile Settings." However, you can control delivery of software and files using a publish-and-subscribe model. For more information, see the *Device Management and File Sync Administrator's Guide.*

Email and PIM Access

After a user connects and passes authentication, the system determines whether the user can access email and PIM information. Wireless Email 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 email and PIM implementation. For more information, see Chapter 8, "Granting Access to the Mail Server."

Nokia Intellisync Wireless Email is a separate product and may not be installed on your server.

Publish-and-subscribe Capabilities

For file delivery, file backup, intranet site delivery, and software delivery, publish-and-subscribe allows the administrator to create a variety of "publication" specifications. You can subscribe groups or individual users to these publications using simple wizard-driven processes in Nokia Intellisync Mobile Suite control.

Delivering Web sites or intranet sites poses an administrative challenge because the Web site may consist of many files spread throughout a complex directory structure. In addition, the links in the pages refer to files on the server. Nokia Intellisync Mobile Suite offers a site-spidering capability that allows the administrator to easily define portions of a Web site. The server scanner packages all associated files for that portion of the site, and "fixes" the links so you can use the links in an offline viewing mode. The same publish-and-subscribe model applies.

The publish-and-subscribe model is the basis of both Nokia Intellisync File Sync and Nokia Intellisync Device Management. For more information, see *Nokia Intellisync Device Management and File Sync Administrator's Guide.*

Enterprise Application Data

Enterprise application databases typically have complex schema, many parent-child relationships, and complex business rules governing user access to subsets of the database relevant to the application. Application Sync provides a tool called Rules Builder that can consider these factors and deliver only the subset of the database that users are authorized to access.

For more information about using Rules Builder to control information access, see the *Application Sync Reference Guide.*

Automated Discovery for New Users and New Devices

When you enable user discovery, any new user with Nokia Intellisync Mobile Suite client and proper network credentials can access the system. Nokia Intellisync Mobile Suite 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 authenticate only devices already in the system.

To set user and device discovery on Nokia Intellisync Mobile Suite control, see "Authentication Tab" on page 36.

Encrypting Communications

Nokia Intellisync Mobile Suite software includes a client component that communicates with the servers through a communications layer.

The following encryption options are available:

- Certicom Based Triple DES—This Data Encryption Standard has 112-bit encryption strength using three 56-bit keys. Nokia does not recommend this option for slow connections or devices with limited processing power.
- Certicom Based AES—This Advanced Encryption Standard uses 128-bit keys, which provides a highly secure connection and is optimized for wireless connectivity.
- Secure Sockets Layer (SSL)—This highly secure option 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.

For more information, see "Configuring Security/Encryption Settings" on page 83.

New Session Keys

For key exchange, Nokia Intellisync Mobile Suite uses Diffie-Helman 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. Diffie-Helman based keys are exchanged every session or on a pre-defined interval in minutes, hours, or days.

Encrypting All Data

Nokia Intellisync 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.

Encrypting User Credentials

Nokia Intellisync always encrypts user credentials as they are passed from client to server for authentication, unless you disable the encryption capabilities. You can specify for the credentials to never expire or to expire after a pre-defined interval in minutes, hours, or days.

Encrypting Staged Files

Nokia Intellisync File Sync and Nokia Intellisync Device Management uses servers that optimize mobile communications by pre-staging information for delivery to authorized users. All information saved in the staging area is encrypted.

Managing User Credentials on the Device

Nokia Intellisync Mobile Suite 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. For more information, see “Configuring User Credentials” on page 84.

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.

Storing User Credentials 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.

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 Nokia Intellisync Mobile Suite products are 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, Nokia Intellisync Mobile Suite works with third-party tools such as Certicom’s movianCrypt.

Managing Passwords

Nokia also recommends effective device password management. For more information, see "Configuring Power-on Password Settings" on page 86.

Requiring a Device Power-on Password

If you have Nokia Intellisync Device Management installed on your server, you can require the user to enter a password to power on the device. You can set the following configurations for different strengths of password protection:

- 4-digit numeric
- 4-digit alphanumeric
- 5 to 40 digit alphanumeric
- 8 to 40 digit alphanumeric (include at least one of each: lowercase, uppercase, numeric, and special characters).

Requiring a Password to Synchronize

If you are unable to store user credentials on the device, you can require the user to enter a password to synchronize.

Device Inactivity Time-out

You can set the following configurations to enforce the device to display a password screen for the user to continue using the device when a device is not used for one of the following time intervals:

- 0 minutes
- 1 minute
- 5 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 1 and 1/2 hours
- 2 hours
- 12 hours
- 24 hours

For more information, see "Configuring Power-on Password Settings" on page 86.

Forgotten Password

You can initiate a randomly generated password to be configured for a device in pre-defined intervals. You can set up how often the forgotten password is generated or refreshed; for example, every hour, every day, or every week. When you initiate a forgotten password sequence, the user will be able to use the password to gain access to the device and perform a synchronization. The user is then prompted to create a new power-on password while the system generates a new forgotten password. For more information, see "To generate a random password" on page 88.

Outgoing Calls

You can define what functions a user can perform while a device is locked. You can restrict everything from allowing only emergency (3-digit) calls to allow specific numbers such as 1-800 numbers, IT support desk, and so on. You can also allow incoming calls using DTMF tones. For more information, see "To configure calling on a locked device" on page 88.

Power-On Password Attempts

The system tracks the number of invalid power-on password attempts a user makes and invokes the appropriate theft/loss protection setting when the maximum number of attempts is reached. For example, the system might

- Deactivate the user
- Delete the PIM and email data
- Delete one or more files
- Hard reset

For more information, see "Configuring Configuration Policy Settings" on page 129.

User Name and Password Attempts

Similar to power-on password attempts, the system tracks the number of invalid user name and password login attempts a user makes to access the system and invokes the appropriate theft loss setting when the maximum number of attempts is reached.

Device Lock

Device lock overrides all other passwords on the device, including the power-on password and the forgotten password. If the device lock password is enabled, the only password you can use to unlock the device is this one. This feature is useful if the device is lost or if the user leaves the company, ensuring that the device cannot be used.

Network Configuration

Network configuration is another key element in your corporate security strategy. There are several options for placing Nokia Intellisync Mobile Suite servers in your company’s network. Refer to Chapter 6, “Network Configuration” for the recommended configuration option. For detailed information on installing and configuring the Secure Gateway, refer to *Nokia Intellisync Mobile Suite Secure Gateway Administrator's Guide*.

6 Network Configuration

Your company policy may dictate how you use Nokia's technology within your network configuration. There are several configuration options available; however, Nokia recommends the configuration described in this chapter using a demilitarized zone (DMZ), or screened subnet. The DMZ is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Recommended Secure Gateway Configuration

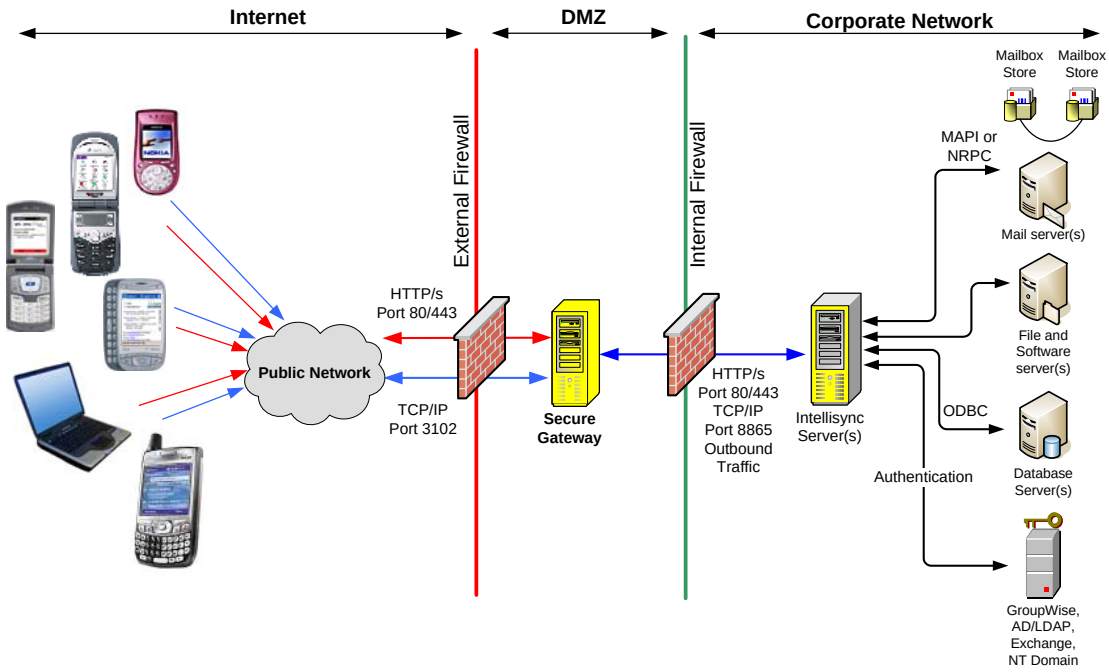
Nokia recommends using the Secure Gateway configuration within your network. The Secure Gateway offers secure and scalable communications between mobile devices and servers and consists of an HTTP listener and communications services.

The Secure Gateway intercepts the HTTP requests from mobile devices to the Intellisync Mobile Suite server and can route the requests in several ways:

- Push requests through TCP/IP port 3102
- Sync requests through ports 80 and 443
- Web requests through ports 80 and 443
- SMS Push requests through port 25

The following diagram illustrates the recommended configuration for the Secure Gateway. In this scenario, all Intellisync Mobile Suite components and enterprise servers are behind the corporate inner firewall.

Figure 7 Recommended Secure Gateway Configuration



The following table shows the default port settings for communication from devices. Your port settings may be different depending on your network configuration

Communication Protocol	Default Port
HTTP • Sync traffic • Web tunneling	80 (configurable)
HTTPS • Sync traffic • Web tunneling	443 (configurable)
TCP/IP Push traffic	3102 (configurable)
SMS Push	25

Note
If your security or firewall policies restrict outbound traffic to the Internet, ask your IT department to establish an outbound rule to allow HTTPS connections over the TCP 443 port to https://ccds.nokia.com.

The following table shows the default port settings for communication from Nokia Intellisync Mobile Suite server. Your port settings may be different depending on your network configuration.

Communication Protocol from the Server	Default Port
HTTP Outbound traffic	80 (configurable)
HTTPS Outbound traffic	443 (configurable)
TCP/IP Outbound traffic	8865 (configurable)

Summary

The Secure Mobile Gateway is a communications infrastructure component of Nokia Intellisync Mobile Suite. Secure Mobile Gateway offers secure and scalable communications between mobile devices and servers.The benefits of this configuration include simplicity, performance, and security.

Simplicity

- The installation application allows you to quickly install and configure the Secure Mobile Gateway.
- A single outbound-initiated TCP/IP port is open in the firewall and you can restrict it to a single IP address.
- DNS routing makes the experience simple whether the client is internal or external.

Performance

- The Secure Mobile Gateway does not significantly reduce performance.

Security

- The Secure Mobile Gateway is highly secure. This configuration securely controls communications between the DMZ and the enterprise.
- This configuration routes traffic to a different protocol and port, thereby restricting any pass-through attempts to the firewall.

For detailed information on installing and configuring the Secure Gateway, referto the *Secure Gateway Administrator's Guide*.

7 Authenticating Users

All users who connect remotely to the Nokia Intellisync Mobile Suite server must be authenticated as a valid user on the server. You can configure Intellisync Mobile Suite 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, Intellisync Mobile Suite authenticates a user by how the user enters the system. For example, Microsoft Exchange users who enter the system through auto-discovery are set up for Windows NT Domain authentication. Lotus Domino users who enter the system through auto-discovery are set up for Domino authentication. Novell GroupWise users who enter the system through auto-discovery are set up for GroupWise authentication. You can change a user's authentication method in Users Properties.

User Authentication Options

There are five approaches to authenticating users with Nokia Intellisync Mobile Suite server:

- Windows NT Domain Authentication (default for synchronization with Microsoft Exchange)
- Domino Authentication (default for synchronizing with Lotus Domino)
- GroupWise Authentication (default for synchronizing with Novell GroupWise)
- LDAP Authentication
- Intellisync Authentication

Exchange Users: Windows NT Domain Authentication

If you import a user from a Windows NT domain or use auto-discovery, then Intellisync Mobile Suite uses NT Domain authentication by default. The user must provide the domain name, user ID, and password to connect successfully. This is the most secure approach for the Intellisync Mobile Suite server (and later accessing the e-mail and PIM server).

For most situations, Nokia recommends Windows NT Domain authentication for Windows NT users.

Lotus Domino Users: Domino Authentication

For Domino users entering the system through automatic discovery, Intellisync Mobile Suite uses Domino authentication by default.When a user connects for the first time, Intellisync Mobile Suite authenticates the user against the Domino server to automatically create a new user account. With other approaches to authentication, you must configure additional options to grant access to the Domino server.

If your system includes email and PIM synchronization (covered in the next chapter), using Domino authentication simplifies the process of granting mail access.

Novell GroupWise Users: GroupWise Authentication

For GroupWise users entering the system through automatic discovery, Nokia Intellisync Mobile Suite uses GroupWise authentication by default. When a user connects for the first time, Nokia Intellisync Mobile Suite authenticates the user against the GroupWise server 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 email and PIM synchronization (covered in the next chapter), using GroupWise authentication simplifies the process of granting mail access.

Intellisync Authentication

With Intellisync Authentication, you are authenticating users against the Intellisync Mobile Suite database. To use this approach, you must have an Intellisync Mobile Suite 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)
- Import users from a text file
- Import users from a list of registered Windows NT users
- Import users from a list of LDAP users

If users need access to an Exchange, Domino, or GroupWise mail server, you must enter additional information to facilitate that connection. For more information on creating new user accounts and adding connection information, see “Working with Users” on page 53.

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

With Intellisync Authentication, the format for a user name is simple. With NT Domain authentication, for example, the domain name must proceed the user name for the user to connect. If you are concerned about having too much network information (such as domain name and log in) available on a device, consider using Intellisync Authentication.

LDAP Authentication

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

If your system includes email and PIM synchronization (as covered in the next chapter), you must use the Exchange courier account to access the Exchange server.

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.

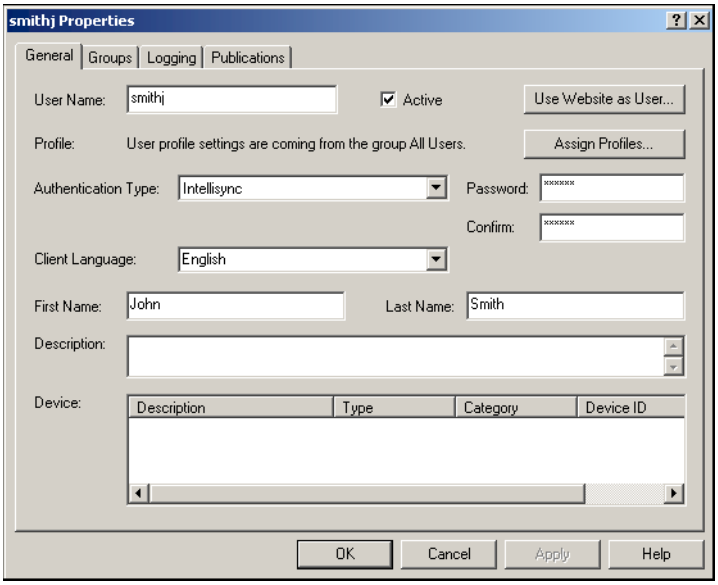
User Entry Source	Default Authentication
Auto-discovery: Windows NT	Windows NT Domain
Auto-discovery: Domino	Domino
Auto-discovery: GroupWise	GroupWise
Imported: Windows NT	Windows NT Domain
Imported: LDAP	LDAP
Imported: other Directory Service	Specific Directory Service
Manually-created: Nokia Intellisync Mobile Suite control	Intellisync Authentication (see note)

Note
Although Intellisync Authentication is the default, you may be able to select NT Domain, Domino, or GroupWise authentication when you create the user.

To view or change a user's authentication source

1. From the console tree, select Management, and then select Users.
2. Select the user you want to change.
3. Choose Action > Properties.

The Properties dialog box appears



Selecting Authentication Types

Windows NT authentication and Intellisync Authentication are available as soon as you install the Intellisync Mobile Suite server software. If you want to use Domino, GroupWise, or LDAP authentication, you must provide more information before you can use these sources.

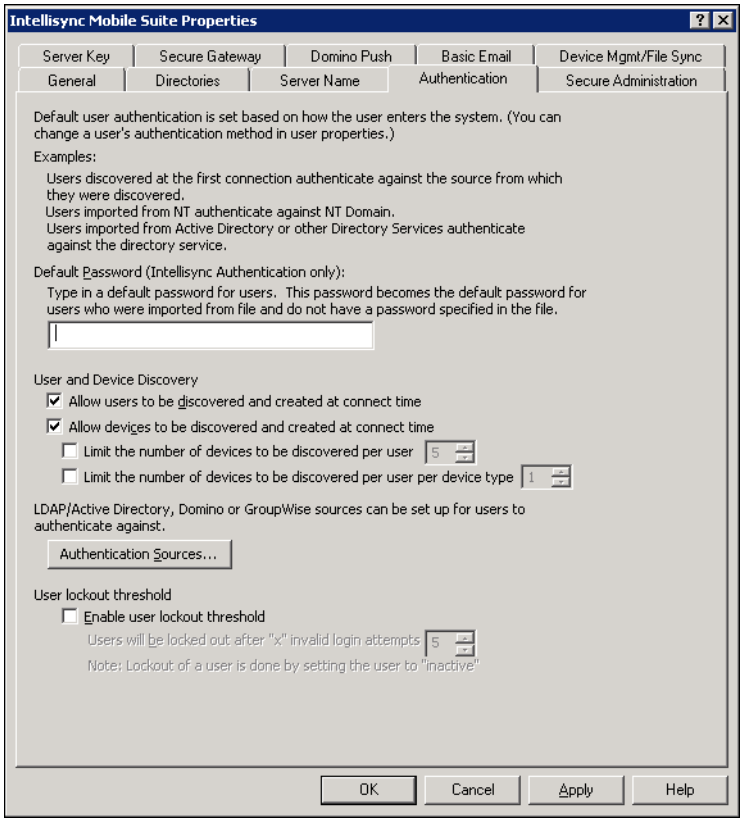
To add Domino, GroupWise, or LDAP authentication sources

1. From the console tree, select Nokia Intellisync Mobile Suite.
2. Choose Action > Properties.

   The Nokia Intellisync Mobile Suite Properties dialog box appears.

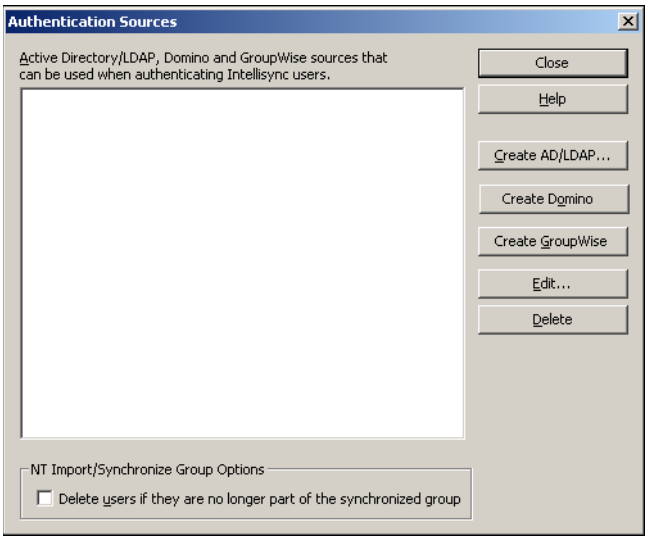
3. Click the Authentication tab.

The Authentication panel appears.



4. Click Authentication Sources.

The Authentication Sources dialog box appears.



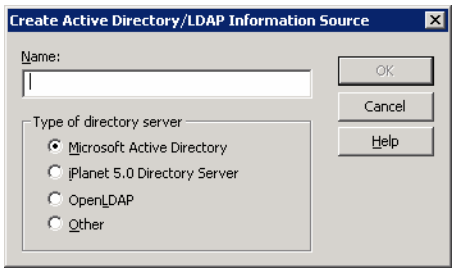
5. Click Create AD/LDAP, Create Domino, or Create GroupWise.

6. Depending on your selection, continue to “Creating an AD/LDAP Information Source” on page 152, “Creating a Domino Authentication Source” on page 154”, or “Creating a GroupWise Authentication Source” on page 154.

Creating an AD/LDAP Information Source

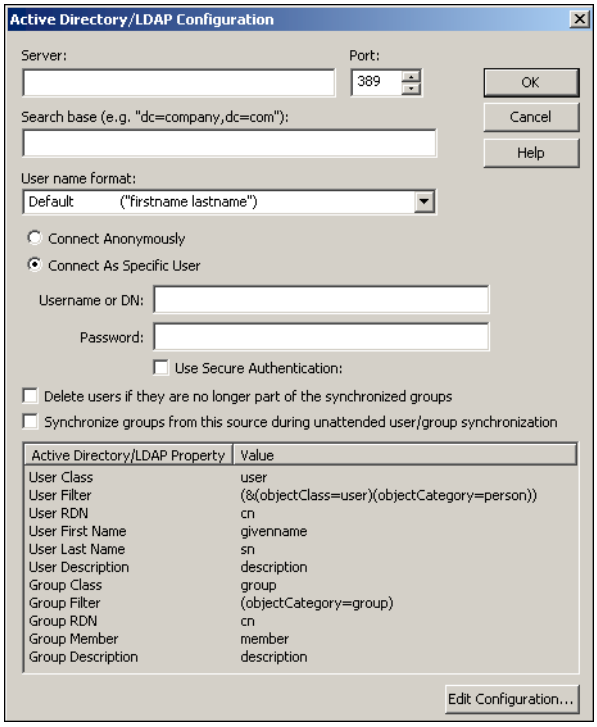
To create an Active Directory/LDAP authentication source

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



2. Complete the fields and select options as necessary, and then click OK.

   The Active Directory/LDAP Configuration dialog box appears.

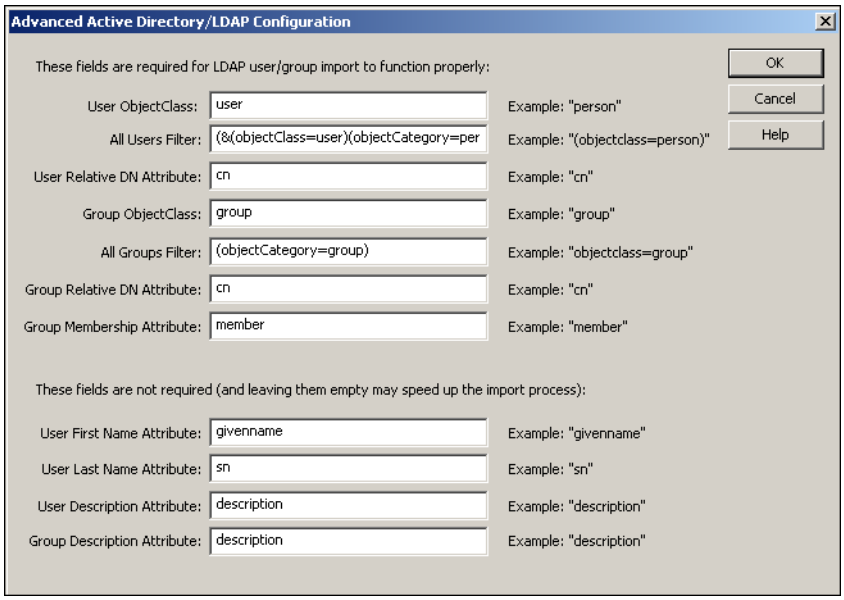


3. Complete the fields and select options as necessary and click OK.

Note
Proceed to step 4 *only* if your LDAP environment uses a User Relative DN Attribute (URDN) value that is different from what appears in the lower portion of the dialog box.

4. To change the User Relative DN Attribute value, click Edit Configuration.

   The Advanced Active Directory/LDAP Configuration dialog box appears.



5. In the User Relative DN Attribute field, enter only “cn” or “userPrincipalName.” Only these values are guaranteed to function properly.

Caution
Do *not* change any other field on this dialog box without first contacting Technical Support.

6. Click OK.

   The Active Directory/LDAP Configuration dialog box appears.

7. Click OK.

   The Authentication Sources dialog box appears.

8. Click Close.

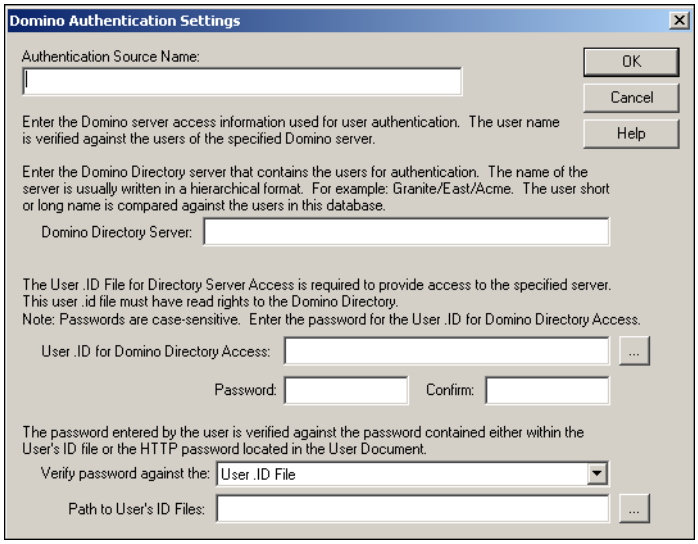
   The Authentication panel appears on the Nokia Intellisync Mobile Suite Properties dialog box.

9. Click OK.

Creating a Domino Authentication Source

To create a Domino authentication source

1. If you clicked Create Domino, the Domino Authentication Settings dialog box appears.

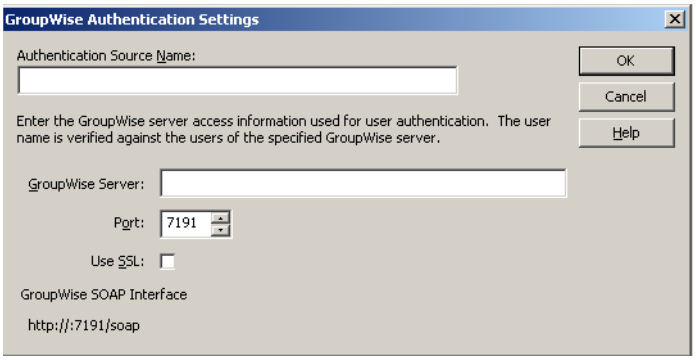


2. Complete the fields as necessary, and then click OK.

Creating a GroupWise Authentication Source

To create a GroupWise authentication source

1. If you clicked Create GroupWise, the GroupWise Authentication Settings dialog box appears.

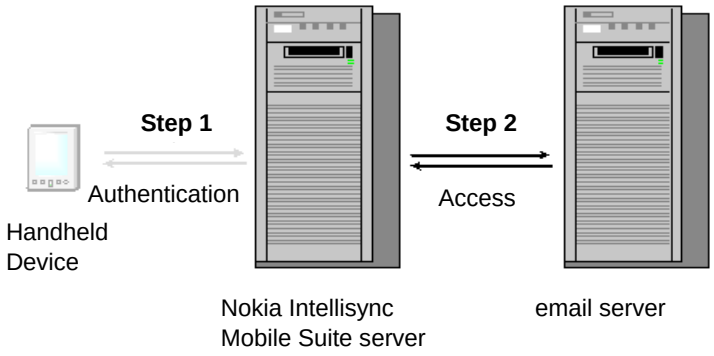


2. Complete the fields as necessary, and then click OK.

8 Granting Access to the Mail Server

All users who connect remotely to the Nokia Intellisync Mobile Suite server must authenticated as a valid user on the server. However, if synchronization for email and PIM data is part of your system, you must grant user access to the mail server.

Figure 8 User Access Between the Device and the email Server



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

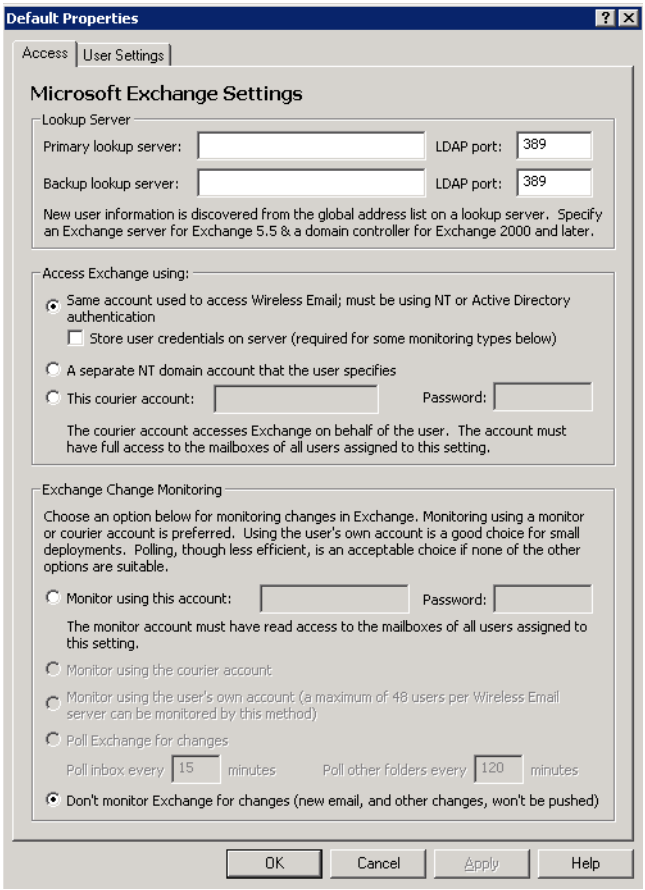
Default profile settings are always in place until you make changes. Therefore, you do not need to create or modify profile settings to start using Nokia Intellisync Mobile Suite.

Note
You must be familiar with Chapter 4, “Profile Settings” before implementing the procedures in this chapter.

Microsoft Exchange: Granting Access to the Mail Server

Wireless Email accesses Microsoft Exchange mailboxes using a Windows NT domain account or a courier account (also a Windows NT domain account). To set up access, create or modify the Exchange profile settings, and then assign the profile to appropriate groups (or users).

1. From the console tree, expand the following:
   - Nokia Intellisync Mobile Suite
   - Profile Settings
   - Wireless Email Settings
   - Microsoft Exchange Settings
2. Select the profile you want to modify.
3. Choose Action > Properties.



For more information, see Chapter 4, “Profile Settings” or the online help.

Accessing Exchange Using a Windows NT Domain Account

Authenticating against a user's Windows NT account is the most secure approach for authenticating with the Nokia Intellisync Mobile Suite server and then accessing the PIM and e-mail server. With this option, Nokia Intellisync Mobile Suite server authenticates users based on the users' Windows NT credentials. To connect, the user must provide the name of the Windows NT domain in addition to the user ID and password.

When a user connects for the first time, the Nokia Intellisync Mobile Suite server automatically creates a new user account based on the user's Windows NT credentials. Therefore, manually creating a user account using Nokia Intellisync Mobile Suite control is not necessary. This feature, called *auto discovery*, automatically discovers the user's mailbox name and Exchange server and adds the user name to the list in the Nokia Intellisync Mobile Suite control. There is no need to manually add information to the properties for the user.

Note
Auto discovery is not available with Nokia Intellisync Authentication. Windows NT authentication is recommended for most situations.

Accessing Exchange Using a Courier Account

If you are using Nokia Intellisync Authentication to authenticate users with the Nokia Intellisync Mobile Suite server, you can access the Exchange server using a courier account. A courier account has full access rights to the Exchange server and every user's mailbox. This account must have service administrator privileges on every Exchange server with which it is synchronized. When a user requests email, this account has the authority to retrieve the user's messages. The same applies when a user requests any other operation on email messages, including deletions. Using Nokia Intellisync Mobile Suite as an intermediary is transparent to the user.

Using a courier account to access the mail server access is simple and easy to manage. This approach is a good choice if you do not want your network information (domain/user ID) available from a mobile device.

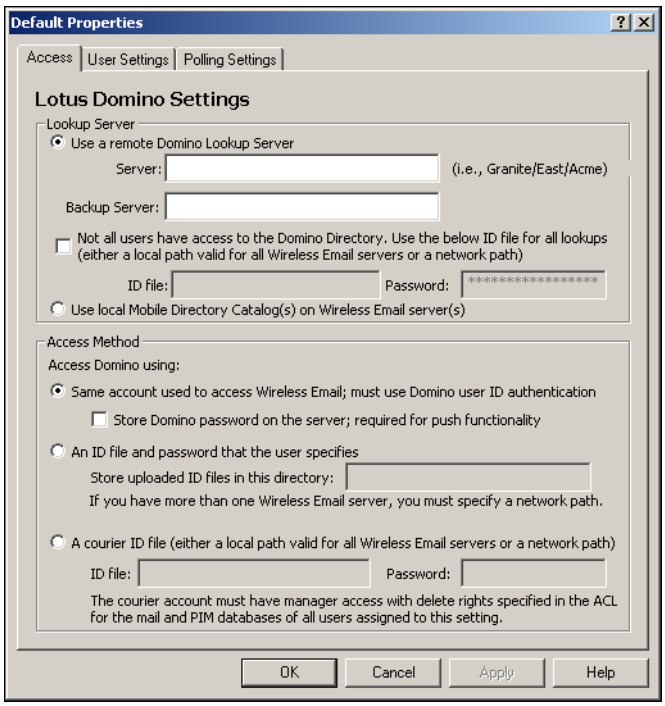
Lotus Domino: Granting Access to the Mail Server

Wireless Email can access a Domino user's mailbox using one of the following options:

- Lotus Notes user ID file
  - Same account used for authentication
  - Different ID file and password specified by user
- Courier account ID file

To set up access for Domino users

1. Create or modify the Domino profile settings, if necessary, and then assign the profile to appropriate groups (or users), as follows:
   a. From the console tree, expand the following:
      - Nokia Intellisync Mobile Suite.
      - Profile Settings
      - Wireless Email Settings
      - Lotus Domino Settings
   b. Select the profile you want to modify.
2. Choose Action > Properties.



For more information on setting these values, see Chapter 4, “Profile Settings” or refer to the online help.

Authenticating Using the Lotus Notes User ID File

Authenticating against the user ID file is the most secure of approach for accessing the Domino server. Auto discovery is an added benefit of this approach.

Using this approach, the Nokia Intellisync Mobile Suite server authenticates against the user’s Lotus Notes ID (*.ID) file to access the user’s mailbox. Then, Nokia Intellisync Mobile Suite automatically creates the user in the Admin Console. There is no need to manually add information to the properties for the user.

In this scenario, all *.ID files for mobile users must be centrally located on a network server instead of (or in addition to) being stored on individual client computers. If storing the *.ID files on a network server is a viable option, Nokia recommends this approach for Domino access.

Each Lotus Notes user ID file is stored locally. If a user changes information such as a password, you must keep track of the changes. You can use Nokia Intellisync File Sync to solve this problem.

The ID file must be the user's Domino shortname. Nokia recommends that the login name match the shortname of the ID file.

Authenticating Using a Courier Account ID File

You can set up a courier (or manager level) account that has read and write access to all mailboxes on the Domino server. To gain access to the Domino server, a user must have the manager account's user ID file in the Access Control List (ACL) of their Domino mailfile.

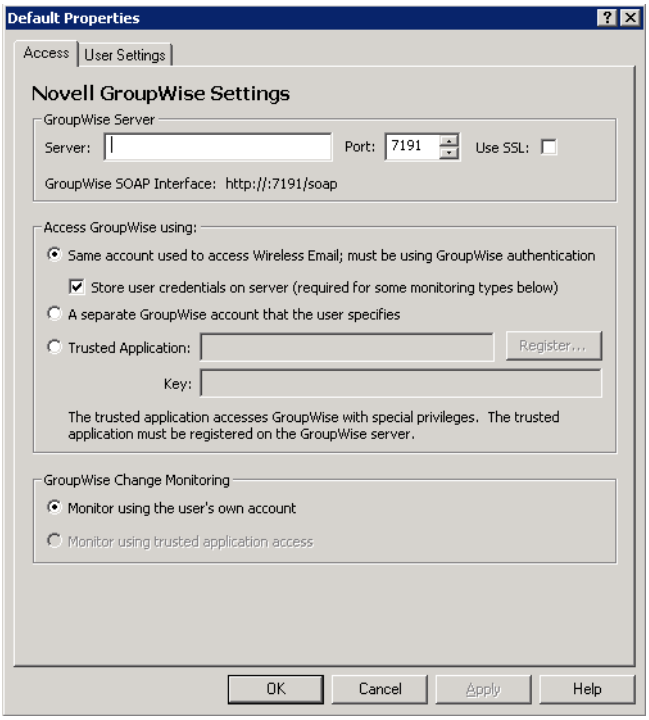
In Courier ID setup, the Courier ID needs to allow manager access to each Lotus Notes mailfile to be synchronized. The Courier ID can be setup as a server ID and can then be added to each user's ACL as a server. Alternatively, the Courier ID can be added to the "LocalDomainServers" group. Adding the ID to this group decreases the impact of installation. Always add this Courier ID as a server, to eliminate the possibility that an unauthorized Lotus Notes client could use this ID to access the system.

Novell GroupWise: Granting Access to the Mail Server

Wireless Email 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:
   - Nokia Intellisync Mobile Suite
   - Profile Settings
   - Wireless Email Settings
   - Novell GroupWise Settings
2. Select the profile you want to modify.

3. Choose Action > Properties.



For more information, see Chapter 4, “Profile Settings” or online help.

Authenticating Using a GroupWise User Account

Authenticating against a user’s GroupWise user account is the most secure approach for authenticating with the Nokia Intellisync Mobile Suite server and then accessing the PIM and email server. With this option, the Nokia Intellisync Mobile Suite server 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 Nokia Intellisync Mobile Suite server automatically creates a new user account based on the user’s GroupWise account credentials. Therefore, manually creating a user account using the Nokia 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 Nokia Intellisync Mobile Suite control. There is no need to manually add information to the properties for the user. Auto discovery is not available with Nokia Intellisync Authentication. GroupWise authentication is recommended for most situations.

Authenticating Using a Courier Account

If you are using GroupWise Authentication to authenticate users with the Nokia Intellisync Mobile Suite server, 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 email, this account has the authority to retrieve the user's messages. The same applies when a user requests any other operation on email messages, including deletions. Using Nokia 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.

Authentication and Access Strategies

When deciding on an authentication and access strategy, it is important to consider your environmental variables. For most situations, Nokia recommends the following strategies.

For Exchange users, consider using Windows NT (domain) authentication between the user's hand-held device and the Nokia Intellisync Mobile Suite server. Then use the user's Windows NT domain account to gain access to the Exchange server.

For Domino users, consider using Domino HTTP access for authentication between the user's hand-held device and the Nokia Intellisync Mobile Suite server. Then, use the Lotus Notes user ID file to gain access to the Domino server. For faster access, without encryption support, you can use a Courier ID to gain acess to the Domino server.

For GroupWise users, consider using GroupWise authentication between the user's handheld device and the Nokia Intellisync Mobile Suite server. Then, use the user's GroupWise user account to gain access to the GroupWise server.

9 Maintaining Nokia Intellisync Mobile Suite

Backup and Restore Overview

It is important to back up your directory structure, files, and data on a regular basis. In addition, it is important that you back up and restore your Intellisync Mobile Suite data in a specific way to ensure that various parts of your system remain in sync.

Always back up your databases and your file system at the same time. If you need to restore your Intellisync Mobile Suite server, be sure to use the database backup and file system backup from the same date and time.

The file system keeps track of data going in and out of the database. Therefore, it is important for the database and file system to always remain in sync.

Backup Procedure

Below is an overview of the backup procedure.

1. Stop Intellisync services.
2. Back up the Intellisync Mobile Suite database.
3. Back up the Intellisync Mobile Suite file system from the install location.
4. Restart Intellisync services.

These steps are covered in more detail in the pages that follow.

Stop Intellisync Services

Stop Intellisync services.

To stop services

1. Choose Start > Programs >Administrative Tools > Services.
2. Select Intellisync Mobile Suite.
3. Choose Action > Stop.

Back Up the Database

Back up the Intellisync Mobile Suite database, according to your company's recommended backup procedures.

Back up the File System

Back up the shared file system for Intellisync Mobile Suite. This is typically \Program Files\Intellisync\PIM\ or \Program Files\Synchrologic\PIM\.

Locate and back up the SharedFileSystem folder.

Restart Intellisync Services

Restart Intellisync services.

To restart services

1. Choose Start > Programs >Administrative Tools > Services.
2. Select the Intellisync Mobile Suite service.
3. Choose Action > Start.

Restore Procedure

Here is an overview of the restore procedure. These steps are similar to the steps for backing up, but with a few key differences.

1. Stop Intellisync services.
2. Restore the Intellisync Mobile Suite database.
3. Restore the Intellisync Mobile Suite file system.
4. Run *SystemRestored.vbs*.
5. Restart Intellisync services.

Stop Intellisync Services

Stop Intellisync services. For more information to complete this task, see "Stop Intellisync Services" on page 163.

Restore the Database

Restore the Intellisync Mobile Suite database, according to your company's recommended restore procedures.

Restore the File System

Copy the shared file system back to its original location on the server. If you accepted the defaults during system installation, the location is \Program Files\Intellisync\PIM\ or Program Files\Synchrologic\PIM\.

Run SystemRestored.vbs

If you followed the backup and restore procedures to this point, your database and shared file system should be in sync. However, the clients may be expecting the Intellisync Mobile Suite server to be in a different state, based on the last time they connected. Running a script called *SystemRestored.vbs* (located in the \PIM directory where the software is installed) helps the server work with the clients to get back in sync.

You can use Microsoft's Cscript utility (located in the WINNT\System32 directory) to run this script.

Note
Run SystemRestored.vbs only after restoring your Intellisync Mobile Suite system from backup as instructed in this chapter. This script is not intended to be used in any other situation or for any other purpose.

Restart Intellisync Services

Restart Intellisync services. If you need more information to complete this task, see "Restart Intellisync Services" on page 164.

Index

F

G

H

I