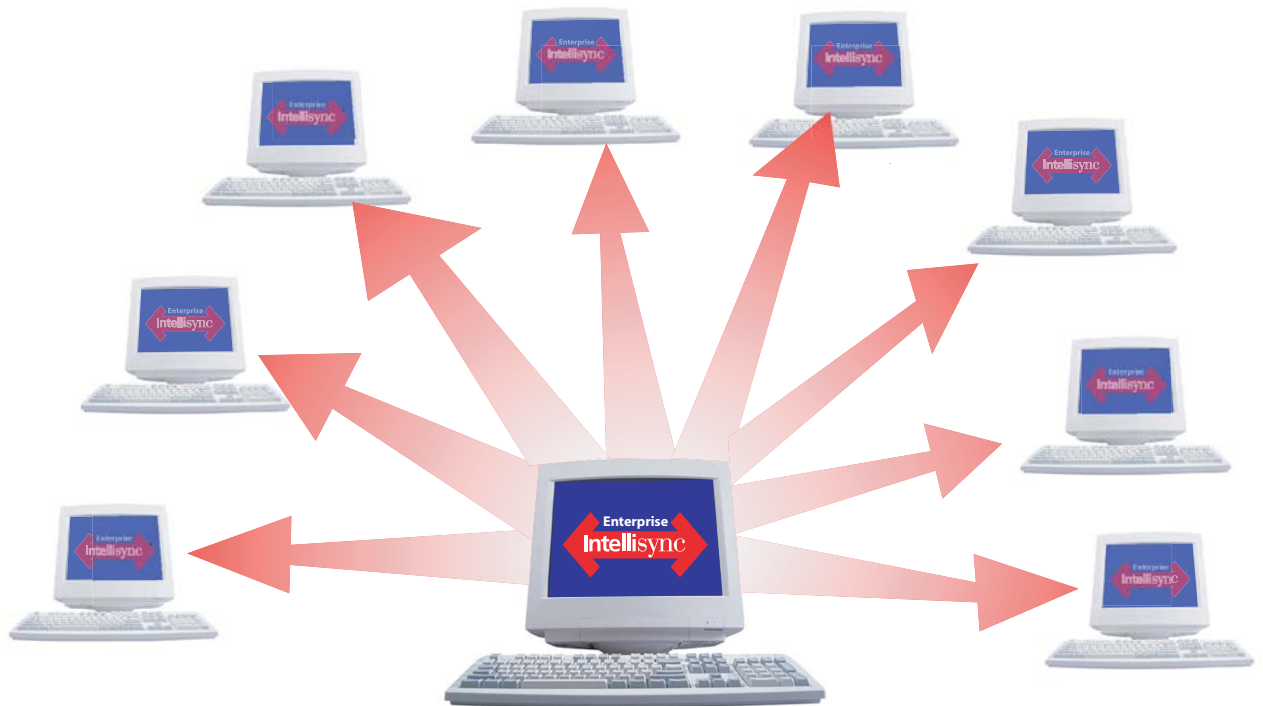




# Enterprise Intellisync™ White Paper

Integrated synchronization  
management for the mobile  
enterprise.





# Introduction

---

This paper describes an evolutionary step in the life of mobile data solutions. These are the software solutions that facilitate sharing of data among a wide variety of mobile devices, while living up to the security and integrity requirements of the enterprise environment. Participating mobile devices may include one or more Microsoft® Windows® personal computers; handheld computers powered by operating systems like Palm OS® or Windows CE; data phones such as the Kyocera smartphones or the Nokia 9000 Series Communicators; and, wireless products like the Research in Motion BlackBerry™ or the Motorola PageWriter™ pager. These are but a few examples of the many devices accessible to consumers and enterprises alike, with applications capable of storing and managing both personal and enterprise information.

*This paper describes evolutionary software solutions that facilitate sharing of data among a wide variety of mobile devices.*

The process of exchanging data between various devices and applications is commonly known as “synchronization”, suggestive of the relentless need to maintain consistent and accurate data across all cooperating elements. The productivity and cost benefits derived from deploying mobile devices within the enterprise have been highly touted and are generally well understood. But the enterprise tools needed to safely harness the power of these devices are ostensibly missing. The strengths and usage characteristics of every device can vary greatly, resulting in the frequent deployment of not just one but several device types. One device may be fit for a given user group, while a second device is better suited for another user group within the same enterprise.

*The enterprise tools needed to safely harness the power of these devices are ostensibly missing.*

Since the equipment manufacturers themselves have little incentive for providing software to help you manage devices supplied by competing vendors, the enterprise is often left with fighting software solutions that reflect a conflicting device bias and parochial view of the mobile universe. This state of software chaos has the unfortunate impact of softening the overall value proposition associated with mobile devices, because it imposes a costly management burden on the enterprise. And few software solutions exist to effectively bridge this gap. Today's solutions tend to fall into one of two broad categories. The first category involves PC-centric software largely targeting consumers, and typically boasting a theme of “the end-user is king”. These standalone products tend to offer few if any management tools to assist in protecting enterprise assets. The second category involves server-based solutions targeting the enterprise, generally aimed at wireless connectivity with mobile devices. Since wireless connectivity to mobile devices has yet to reach the mainstream, these solutions tend to be underused. They often lack integration with

*Today's solutions tend to fall into one of two broad categories - PC-centric software and server-based solutions.*

crucial desktop components and established tools that could otherwise ease the management burden inside the enterprise.

*Mobile appliances are fast becoming embedded in the core fabric of enterprise applications.*

But the mobile landscape is changing. Not long ago considered renegade devices, mobile appliances are fast becoming embedded in the core fabric of enterprise applications. Gartner Group, Inc. projects a PDA (Personal Digital Assistant) population of 20 million users by 2003, primarily installed in the enterprise. In turn, this is forcing the software solutions themselves to evolve. New products expressly designed for the enterprise are arriving on the scene, promising to integrate mobile capabilities into established management consoles. Thus, mobile solutions are finally joining the arsenal of essential management tools, reflecting a growing recognition that “the enterprise is king”. This doesn’t mean that the end-user has suddenly become unimportant. Rather, it means that the enterprise finally has access to mobile tools that can better serve the diverse needs of its constituents without compromising corporate goals. We’re entering the era of centralized management, where mobile software is brought back into the enterprise fold and managed like the valuable asset that it is.

*Enterprise Intellisync offers a here-and-now solution that lets the enterprise immediately regain control of the weakest link in the chain - desktop-based mobile software.*

As a recognized leader in the area of data mobility, Pumatech introduces **Enterprise Intellisync**. This innovative product aims to turn out-of-control devices into secure appliances within the enterprise environment. The product combines the advantages of its award-winning Intellisync application with central management features to assist administrators in tailoring and controlling the mobile solutions deployed in the corporation. It offers a here-and-now solution that lets the enterprise immediately regain control of the weakest link in the chain - the mobile software running on every desktop. And it integrates with popular enterprise applications like the Microsoft Management Console (MMC) and Microsoft Systems Management Server (SMS).

Using Enterprise Intellisync, the administrator is empowered with all the tools necessary to centrally manage the deployment and ongoing maintenance of Intellisync. The product includes all the features required to manage user licenses, configure end-user software settings, enforce feature restrictions by user group, deploy and upgrade mobile desktop software, and troubleshoot end-user problems as they occur. And this is all done from a central console.

In summary, Enterprise Intellisync is an integrated management tool that places mobile control back in the hands of the enterprise, thereby improving the return on investment in mobile devices and software. Gartner Group, Inc. estimates that the total cost of ownership (TCO) for a PDA deployed in the enterprise approximates \$2,800 per year. This is a relatively high cost when compared with the average capital cost of \$450 for the PDA itself. Enterprise Intellisync aims to directly reduce the TCO by providing the tools needed to manage PDAs like corporate assets.



## It's All About Control

---

The enterprise has been at a severe disadvantage in the fight to control the onslaught of mobile devices. The under \$500 price tag often tempts employees to expense them after-the-fact, or to simply pay for the device themselves. But reliable studies have shown the total cost ownership to be 10 to 20 times the initial price of the mobile device itself. When the cost of software, maintenance and troubleshooting is added to the price tag, it becomes clear that mobile devices are not inexpensive gadgets. So, it's no surprise that getting them under control is fast-becoming a priority issue in the enterprise. The cost-effectiveness of these devices hinges on their ability to aid productivity without infringing on enterprise policies and systems. So, what is it that really needs to be "controlled"?

*The total cost of ownership for a mobile device has been shown to be 10 to 20 times the initial price of the device itself.*

a) **Applications.** Most mobile devices come bundled with a desktop application that provides connectivity services for that device. These applications vary by manufacturer and are mainly designed with the consumer in mind. This means they offer little assistance to the enterprise in the way of managing their usage. But the fact that they're included in the package makes them popular with end-users, since no additional out-of-pocket expense is required to use them. Unfortunately, what's convenient for the end-user is not necessarily the most effective solution for the enterprise as a whole. Thus, the first mobile element that needs to get under control is the choice of desktop application to deploy with sanctioned mobile devices. For manageability reasons, it's necessary to establish and deploy consistent applications, regardless of the freebies in the box. And the selected applications must be friendly to the enterprise such that they help rather than fuel the existing mobile management problem.

*For manageability reasons, it's necessary to establish and deploy consistent applications, regardless of the freebies in the box.*

b) **Licenses.** Once the mobile applications have been selected, the administrator needs to determine who in the enterprise will have access to these applications. This is best accomplished using a user licensing mechanism built directly into the software. In that way, licenses can be centrally issued and administered. Only in this way can the enterprise remain truly in control of who has what mobile software.

c) **Functionality.** When it comes to mobile applications, the "one size fits all" philosophy definitely does not apply. An enterprise typically employs some lightweight users, some advanced users, and varying degrees in between. So, the notion of exposing the same features and user interface

across all user groups risks putting too much horsepower in the hands of some, and not enough in the hands of others. The enterprise needs to be in control of assigning functionality levels to user groups based on actual need. And it shouldn't be necessary to revert to multiple applications to do it. Enterprise-friendly mobile solutions can provide the management tools necessary to enable and restrict application features based on user profiles.

*If each user is left to the task of manually installing the application, the enterprise loses control.*

d) **Installation.** After the user licenses have been issued, the mobile application has to be deployed and installed on each desktop computer. The enterprise needs to control the actual deployment of the application, and should be able to complete the installation remotely without visiting each desktop computer. If each user is left to the task of manually installing the application, the enterprise loses control. Note that industry-proven tools already exist to remotely install desktop software. The mobile tools aren't expected to duplicate this functionality, but rather to integrate with well-known software management systems installed.

e) **Upgrades.** All upgrades to the mobile applications need to be placed under the control of a central administrator, just like the initial installation. Otherwise, the enterprise risks higher support costs resulting from supporting old software releases or from "bleeding edge" versions that have not yet been tested. To be effective, upgrades also need to respect the user license that was issued prior to the initial installation. In addition, the administrator should have the ability to designate how the prior user settings are affected during the upgrade.

*The enterprise must have control over the content of the configuration, with possible variations in settings between user profiles.*

f) **Settings.** Every application includes "user settings" that influence the behavior of the installed software. Some settings are innocuous, while others can have a more significant impact on the operation of the software. If not controlled, the user configuration (combination of settings) can become problematic, resulting in higher support costs for the organization. For these reasons, the enterprise must have control over the content of the configuration, with possible variations in settings between user profiles. The administrator should have the flexibility to create default configurations by user group, and if necessary, be able to prevent users from changing or even seeing certain settings altogether.

*The administrator needs the flexibility to mandate that users supply a password whenever entering the desktop application.*

g) **Security.** Most consumer-centric applications either make security an optional feature to be set by the end-user, or make no security provisions at all. In the enterprise environment, security is a prerequisite feature assumed to be present in any robust application. And the responsibility for establishing security rules and privileges rests with the administrator rather than the individual end-users. For example, the administrator needs the flexibility to mandate that users supply a password whenever entering the desktop application. Likewise, he or she should have the ability to grant or deny end-users the right to change application passwords. Security is a crucial mobile element that belongs in the hands of an administrator.

h) **User Help.** The effort and cost involved in supporting standalone mobile applications can be quite significant. This is partly due to the fact that

non-integrated applications normally require a support specialist to visit the desktop computer that's experiencing the problem. And once at the desktop, the nature of troubleshooting can vary depending on the particular application installed. It's time to place problem analysis and troubleshooting under central control. For example, it should be possible for end-users to send problems and associated details in electronic form to an administrator for analysis. Mobile solutions need to include the prerequisite tools for managing end-user problems.



# Taming the Cost of Ownership

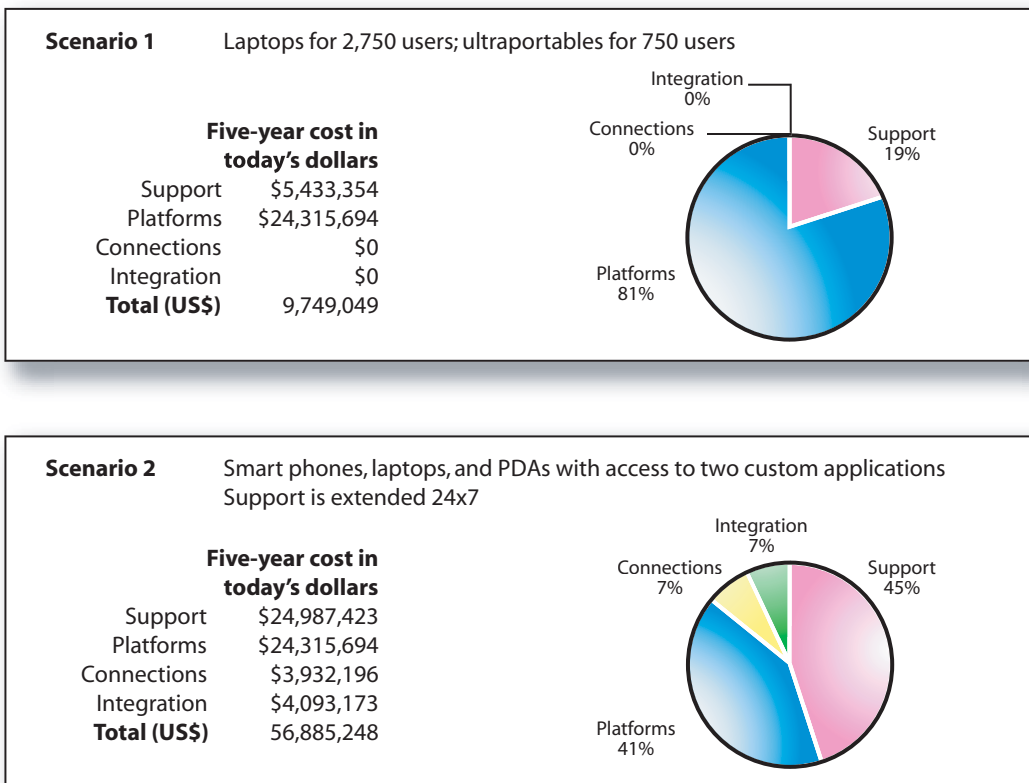
*The acquisition cost of the initial hardware and software is generally modest, but there are significant hidden costs in the area of support.*

The total cost of ownership (TCO) for mobile devices and software is much higher than suggested by the retail price of the device alone. The acquisition cost of the initial hardware and software is generally modest, but there are significant hidden costs in the area of support. This is particularly true in the enterprise, where hundreds or thousands of different devices may be deployed across geographical locations. Gartner Group, Inc. estimates that the TCO for a Palm OS-based PDA is nearly \$2,700 per year. Similarly, they estimate a TCO of around \$2,800 for a Windows CE-based PDA. Although the acquisition cost of the average PDA is in the range of \$450, the TCO ends up being 7 times the capital expenditure each and every year. And if we assume the PDA to have a three-year life, its TCO exceeds 18 times the capital cost! (Figure 1 shows the potential significant cost increases of supporting PDAs in the enterprise - a 5-6 times cost increase over 5 years.) The enterprise desperately needs ways to reduce the TCO. Only then can they begin to fully reap the long-awaited benefits that we all believe are possible. There are many opportunities for reducing the TCO of mobile solutions:

- a) Bulletproof the installation and maintenance of the mobile software at the desktop. This reduces the likelihood of startup problems, and can eliminate wasted time on the part of both the support team and the end-users.
- b) Eliminate the need for frequent visits to the desktop by support personnel. Management tools that support remote deployment and administration can go a long way toward reducing the need for onsite support calls.
- c) Reduce training costs for both the support staff and end-users. Integrated tools for the administrator and a simple user interface for the end-user are key elements needed to lower training time and costs.
- d) Limit exposure to software functionality based on the specific needs and sophistication of each user group. For example, restricting access to advanced features that are not necessary, or allowing them to be preset and locked by an administrator, can eliminate various sources of support problems.
- e) Lower end-user downtime by speeding up problem analysis and resolution. Even with the best-laid plans, unexpected problems will inevitably arise. The key is to reduce the time span between problem occurrence and resolution.

In order to pursue the cost-reduction opportunities outlined above, the enterprise needs management tools that collaborate (and are integrated) with the mobile applications. These tools target the administrator as their primary audience rather than the end-user. They provide automated assistance in the areas of user manage-

Figure 1. Taken from  
"The Real Cost of  
Mobility", 5/2001,  
Forrester



(numbers have been rounded)

ment, configuration management, installation management, problem management, and change management. These functions are well understood by the enterprise, and have been routinely applied for years to various categories of software. However, it's only been recently that mobile solutions have been subdued into embracing these same functional areas.

\* \* \* \* \*

So, what kinds of management tools are needed to effectively reduce TCO? These tools must be cognizant of the special circumstances surrounding mobile users, while respecting the enterprise goal to maintain centralized control. To be effective, the resulting solution needs to exhibit the following key characteristics:

**Centralized.** The tools must provide administrative control over the deployment and maintenance of mobile applications. Without centralized tools, it's simply not possible to substantially bring down the TCO.

**Integrated.** The various elements need to be integrated under a single console to achieve synergy. For example, the user manager must be integrated with the installation manager to ensure that the deployed software upholds the user license.

**Simple.** The console interface for the administrator as well as the application interface for the end-user must be simple. Complicated and non-intuitive interfaces work against the basic goal of saving time and effort.

**Flexible.** The tools must be capable of supporting the wide range of end-

users who typically coexist within the enterprise. For example, it should be possible to vary the configuration settings and access privileges by user group.

**Extensible.** It should be possible to introduce new administrator and end-user features over time, without necessitating a complete re-installation of software. For example, adding support for a new mobile device or desktop application should require only an update to existing installations.

**Compliant.** The mobile management tools must integrate well with existing systems to protect enterprise investments. This includes tools such as the Microsoft Systems Management Server (SMS) and the Microsoft Management Console (MMC). And the desktop tools should integrate with de facto standard software like Palm HotSync® Manager and Microsoft ActiveSync.



## Back to Home Central

---

It's time to get out of the mobile dark ages. The heyday of the standalone mobile application that's picked and installed at the whim of each employee is over. History has shown that the proliferation of these runaway applications results in high support costs. And we need to stop treating mobile devices like exceptions to corporate standards, and start folding them into the established infrastructure of the enterprise. There's a push to centralize the deployment and management of mobile applications, with the following benefits expected to accrue over time:

*We need to stop treating mobile devices like exceptions to corporate standards, and start folding them into the established infrastructure of the enterprise.*

- a) **Less support time at the desktop.** The existence of centralized tools means that the administrative staff can perform more support functions remotely, lessening the need to visit the desktop location. This factor makes an immediate and significant impact toward reducing the overall cost of support.
- b) **No employee time for setup.** Given the appropriate administrative tools, pre-configured applications can be deployed "silently", requiring little or no intervention on the part of the end-user. This not only saves employee time, but also tends to bulletproof the installation. And a bulletproof application exhibits lower startup problems and ongoing support costs.
- c) **Shorter time to diagnose problems.** The availability of centralized tools is key for speeding up the turnaround time on problems. When software anomalies do occur at employee locations, the administrator is able to analyze the problem and accompanying details from a central console. These tools offer more detailed information than ever, further reducing the number of visits to the desktop.
- d) **Rapid software distribution.** Centralized software distribution tools make it possible to install and upgrade desktop applications remotely. The mobile applications can be installed "hands free", and pre-configured for each user. Software releases can be deployed to all employees quickly, reducing both the installation time and the number of concurrent releases to support.
- e) **Lower training costs.** Integrated management tools means that system administrators have less to learn. A single console application with a consistent user interface eliminates the hassle of jumping between disparate

applications. And a plug-in architecture makes it easy to add new components over time. Similarly, deploying a standard desktop application simplifies user training.

f) **Increased security.** Mobile management tools make provisions for centrally controlling software security. This means that a system administrator, in line with corporate policies and procedures, sets user privileges and security policies. Centralized tools afford the enterprise better protection over its mobile assets.

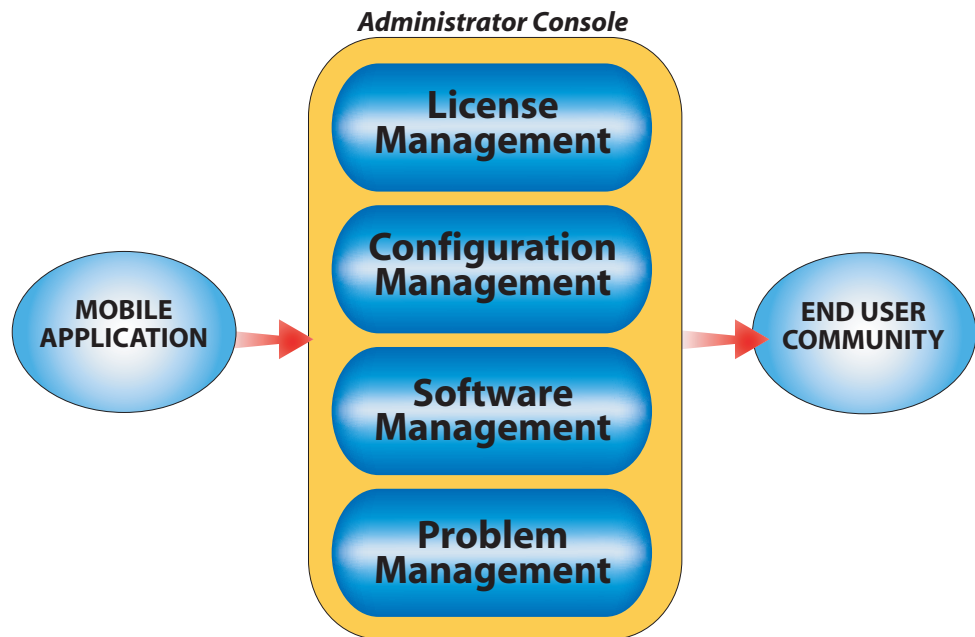
g) **Fewer desktop applications.** By its very nature, centralized control tends to discourage the use of standalone applications in favor of deploying standard software. This leads to economies of scale in both the deployment and ongoing support of applications installed on employee computers.

h) **Single user interface.** Centralized management tools typically operate under a console application, sporting a common user interface across functions. Likewise, deploying a standard desktop application has the benefit of providing a common user interface for all end-users. A single user interface paradigm exists, which simplifies both learning and operating the software.

*When evaluating mobile management tools, it is important to keep in mind that they need to cover several functional areas.*

When evaluating mobile management tools, it's important to keep in mind that they need to cover several functional areas. And these functions must be integrated in order for the enterprise to benefit from their synergy. So, what management components are required to control the deployment and maintenance of mobile applications?

*Figure 2. Four pillars of mobile management*



1. **License Management.** The system administrator needs central tools to create and deploy user licenses with the mobile applications. In effect, the user license is an accounting record that legitimizes access to the given application. These licenses are then enforced by the other components.

2. **Configuration Management.** The tools must allow the administrator to configure application settings on behalf of end-users. This includes granting security privileges, restricting access to features by user group, and setting various application options. The configuration is then delivered to the desktop computers using the software management piece.

3. **Software Management.** This component is responsible for deploying mobile applications on end-user computers, installing software upgrades, and delivering the configuration that corresponds to the end-user. The software management piece should also integrate well with industry-standard applications that more fully address software distribution.

4. **Problem Management.** The problem management component enables end-users to quickly report problems to the administrator, and send an automated record of detailed activities to help isolate the problem. This piece needs cooperation from the mobile desktop application, which is responsible for logging diagnostic information on end-user computers.



# Introducing Enterprise Intellisync

---

*Enterprise Intellisync from Pumatech is expressly designed to help Fortune 1000 companies gain control over the growing number of mobile devices entering their secure environment.*

Little automation was previously available to help the enterprise cope with the invasion of mobile devices and applications. Enterprise Intellisync from Pumatech is expressly designed to help Fortune 1000 companies gain control over the growing number of mobile devices entering their secure environment. It targets the system administrators who manage desktop computers, and end-users who need an easy-to-use synchronization solution that conforms to enterprise standards. The product gives administrators the tools necessary to centrally administer their Intellisync® desktop applications, resulting in deployed solutions that mirror (rather than defeat) corporate policies and budgets. While standalone mobile applications tend to harbor security and control risks, Enterprise Intellisync bulletproofs the solution to reduce TCO and protect the corporate investment. In short, the product was designed with these simple principles in mind:

**Only administrators have the key.** Enterprise Intellisync empowers the administrator to stay in control of all elements of the deployed solution. Only they can issue user licenses, security rules, feature access, and user configurations. This is essential for avoiding mobile mayhem in an enterprise setting.

**Not all users are created equal.** The enterprise normally services various classes of personnel, ranging all the way from casual to advanced users. Enterprise Intellisync builds in the flexibility to address their diverse needs, without baffling the lightweight user or crimping the needs of the sophisticated mobile user.

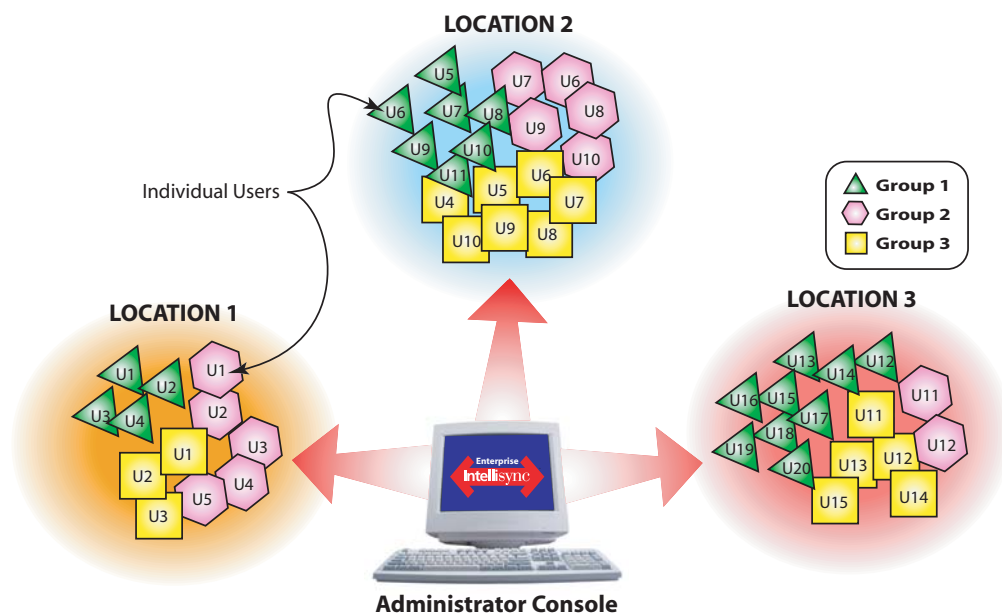
**Simplicity is golden.** Using the deployed applications is a breeze. Enterprise Intellisync makes it possible to fully pre-configure the Intellisync desktop applications, leaving the user to do nothing except “sync”. An effortless user experience reduces the likelihood of problems and lowers support cost.

**No application is an island.** Mobile applications can no longer divorce themselves from other corporate standards. Enterprise Intellisync offers integration with industry-standard applications, wherever possible. This leverages the power of installed tools and protects the investment in corporate infrastructure.

*Enterprise Intellisync comprises two major applications - a console application and a desktop application for end-users.*

Enterprise Intellisync comprises two major applications: (1) a console application, which hosts the management tools used by the system administrator; and (2) a desktop application for end-users, which performs synchronization between various applications and devices. It's the combination of these applications that creates a

bulletproof environment for deploying mobile solutions inside the enterprise. The administrative tools provide the means to manage user licenses, centrally configure the desktop application, remotely distribute and maintain the desktop software, and electronically manage application problems that arise during normal operation.



*Figure 3. Enterprise Intellisync is made up of a console component and a desktop component.*

Consistent with its enterprise focus, Enterprise Intellisync meticulously supports the major groupware applications most frequently licensed by Fortune 1000 companies. At time of product launch, Enterprise Intellisync already supports synchronization with Microsoft Exchange Server, Lotus Domino and Novell GroupWise. Supported devices initially include those powered by Microsoft Windows, Palm OS and Windows CE. These combinations are sure to satisfy the most frequent requests received from enterprise customers. But it doesn't stop there. Enterprise Intellisync implements a plug-in architecture that makes it easy to add new applications, devices, and features over time. And Pumatech is already busy working on the next extensions to this product.

*Enterprise Intellisync implements a plug-in architecture that makes it easy to add new applications, devices, and features over time.*

By design, Enterprise Intellisync is tightly integrated with the Microsoft Management Console (MMC), so as to leverage and extend familiar management tools inside the enterprise. It also provides integration with various software distribution systems, including optional integration with the Microsoft Systems Management Server (SMS). Other management systems from companies like Tivoli, Novell and Computer Associates can also be supported. The Enterprise Intellisync Administrator Console runs under Microsoft Windows NT and Windows 2000. The application also requires Microsoft Internet Explorer 5.0 (or later) and Microsoft Internet Information Services.

*By design, Enterprise Intellisync is tightly integrated with the Microsoft Management Console (MMC), so as to leverage and extend familiar management tools inside the enterprise.*

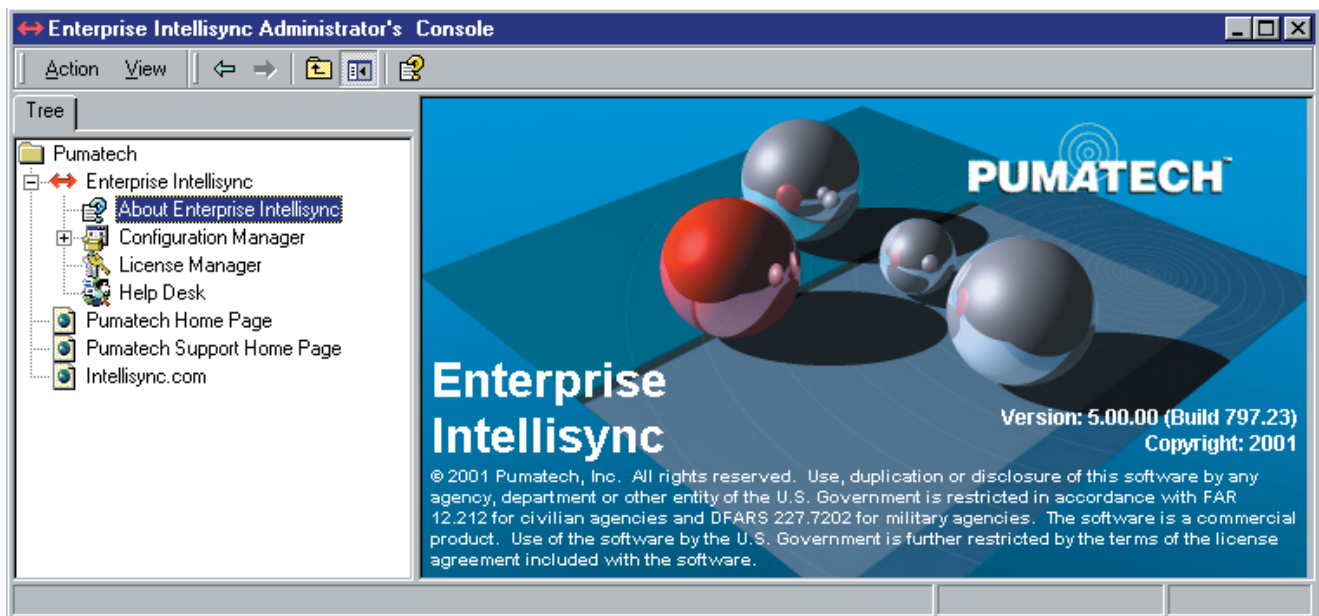
The Enterprise Intellisync desktop application runs on all popular flavors of Microsoft Windows, including Windows NT, Windows 95, Windows 98, Windows 2000 and Windows Me. When using Palm OS devices, Palm HotSync Manager 3.0 or later must be installed on the desktop. For desktops connecting to Pocket PC and Windows CE devices, Microsoft ActiveSync 3.1 or later is required.

# 6

## The Enterprise Intellisync Administrator Console

*This console is the hub through which user configurations, licenses, security rights, and features are assigned and controlled by the system administrator.*

*Figure 4. The components of Enterprise Intellisync.*



*The Enterprise Intellisync Administrator Console runs under the Microsoft Management Console application (MMC).*

The Enterprise Intellisync Administrator Console runs under the Microsoft Management Console application (MMC). MMC is a Windows-based, extensible console framework for managing applications structured as components called “snap-ins”. The MMC doesn’t perform administrative functions on its own, but rather hosts tools that do. This approach eliminates the need to hunt for administrative tools, and lowers the cost of managing Windows-based environments. It provides a uniform, integrated, and familiar environment for administrators to carry out management functions. The Administrator Console is implemented using these MMC snap-in modules:

1. **About Enterprise Intellisync.** The simplest of the MMC snap-ins, this component serves mainly to identify the software version and build number.
2. **Configuration Manager.** The Configuration Manager gives the administrator the

ability to create or change application settings centrally, affecting the behavior of the deployed desktop application for a given user or user group.

3. **License Manager.** As the name implies, administrators use the License Manager to create and issue software licenses. These licenses are then deployed along with each copy of the desktop software to authorize usage.

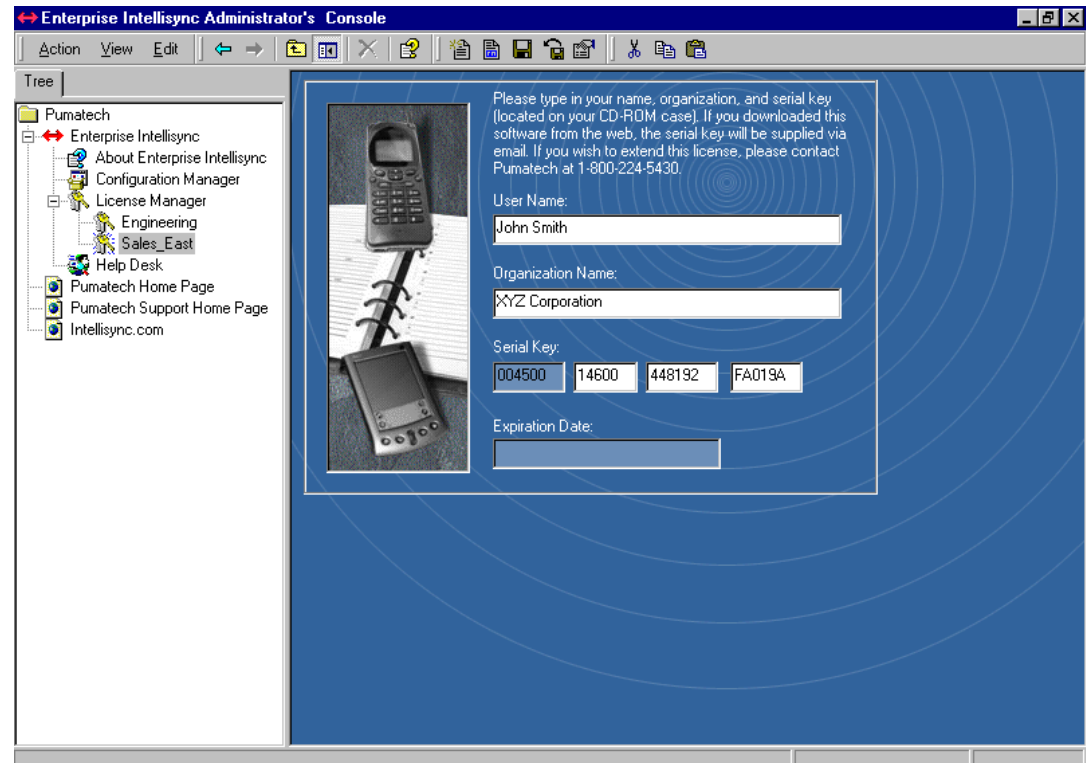
4. **Help Desk.** The Help Desk component allows the administrator to receive and analyze details concerning problems experienced on end-user computers. Intellisync Desktop cooperates with the Help Desk in logging activities.

The snap-in architecture of Enterprise Intellisync and MMC facilitates adding new mobile devices, applications and features over time - all controlled from the same Administrator Console. The product is designed using an extensible model that effectively protects the corporate investment in management infrastructure. Next, we look at how Enterprise Intellisync deals with each of the management functions that are central to administering mobile solutions deployed in the field.

### License Management

Enterprise Intellisync enforces user licenses to control access to Intellisync Desktop clients installed on end-user systems. The License Manager is responsible for ensuring that all distributed desktop elements are legitimate and authorized for use. Toward that end, a device-specific license file must be deployed before the Intellisync Desktop application can be installed or used. The License Manager component is used to create, change and deploy these license files. Once a license has been deployed, it can also be changed centrally and upgraded remotely in the field. For example, the administrator can upgrade from a trial license to a full license, without the need to re-install any software. The License Manager provides central enforcement of license agreements, remote deployment of licenses on end-user systems, and easy, inexpensive license upgrades.

*The License Manager is responsible for ensuring that all distributed desktop elements are legitimate and authorized for use.*

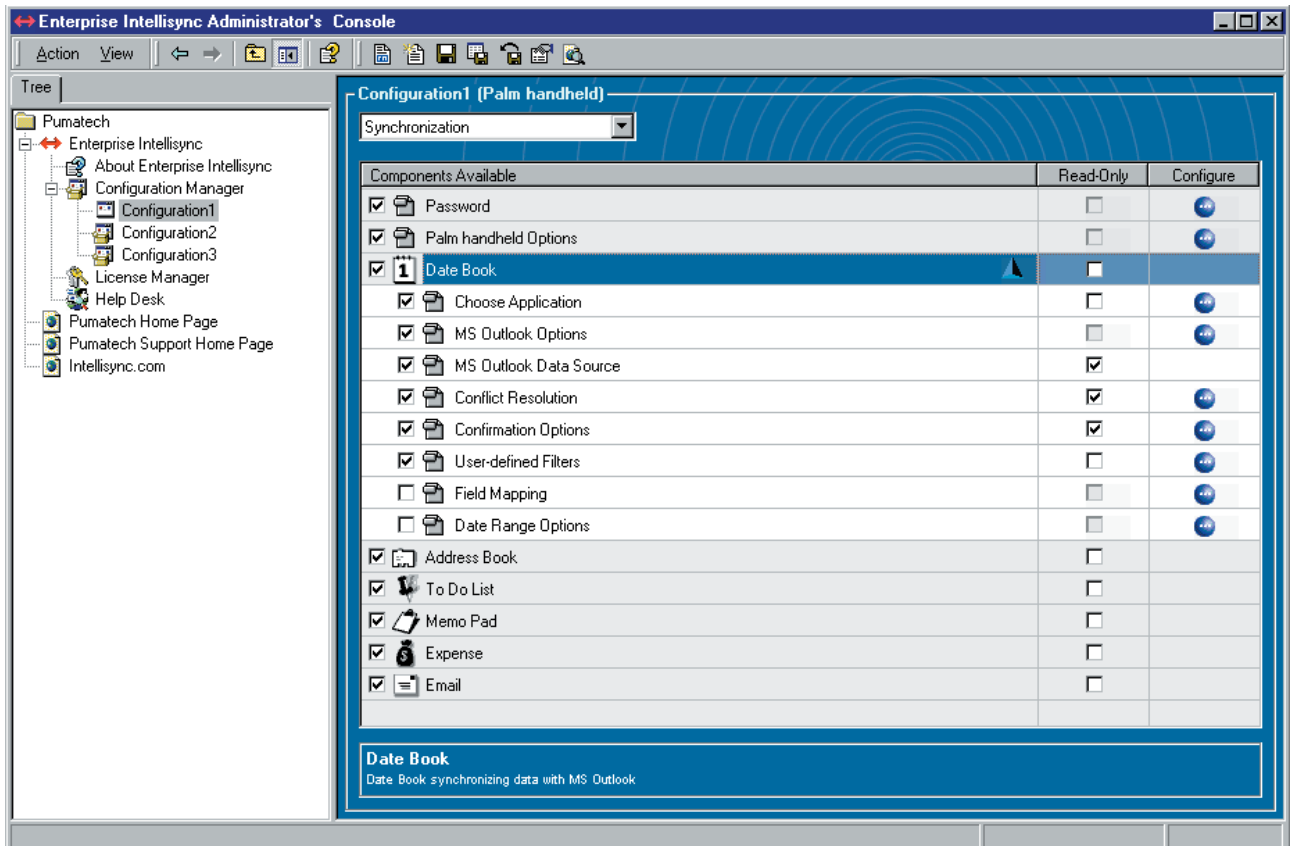


*Figure 5. The License Manager*

## Configuration Management

Enterprise Intellisync gives the administrator full control over the user configurations deployed on desktop computers. A “configuration” is essentially a combination of software settings, user options and access privileges, which collectively influence what the user sees and can do when running Intellisync Desktop. The Configuration Manager offers an unprecedented degree of flexibility toward supporting a wide diversity of companies and end-users. Whereas, most desktop applications tend to “bare all” features to its users, the Configuration Manager provides the means for adapting desktop functionality to the unique requirements of specific user groups.

Figure 6. The Configuration Manager



A primary objective of Enterprise Intellisync is to simplify the synchronization experience for end-users.

A primary objective of Enterprise Intellisync is to simplify the synchronization experience for end-users. The Configuration Manager plays a pivotal role in meeting this objective. The administrator creates user profiles from a central console, reducing or eliminating the need for configuring the mobile application at the desktop. This simple “install and run” approach greatly reduces problems and lowers support costs. The Configuration Manager provides control over the following desktop elements:

a) *Password Protection*. The administrator can choose to enable password protection over the configuration data itself. In effect, this prevents unauthorized personnel from modifying the user configuration on the desktop. Various options exist for controlling password assignment. The password can either be preset by the administrator or first assigned at the desktop by individual end-users. It's also possible to prevent changing the password on the desktop at all, in cases where the password has been “fixed” by the administrator. These options give the administrator the flexibility needed to properly reflect corporate policy.

b) *Device Options*. Each user configuration is associated with a mobile device, such as a Palm or Windows CE device. The administrator can preset any device-specific options from the central console. Examples include setting limits on the size of email text sent to the mobile device, and the treatment of email items deleted on the device side. Once deployed, the device options will impact the result of synchronization operations on the desktop.

c) *Application Settings*. A rich set of options is available to affect synchronization between the mobile and desktop applications. Selecting the desktop applications, database names, field mapping, record filters and conflict resolution rules are examples of the many options that can be preset by the administrator. These and other options are described in greater detail in “The Enterprise Intellisync Desktop” section later in this paper.

d) *Access Privileges*. The Configuration Manager gives the administrator the ability to choose which application components are exposed to end-users. And the choice of visible functionality can also vary widely by user group. In this way, users see only the features they need, thus simplifying the overall user experience. By default, all Intellisync Desktop components are enabled and made visible. However, the administrator can choose to remove, hide or prevent user changes to almost any application component or sub-component. For example, it’s possible for the administrator to remove email from the list of applications the user may synchronize. It’s also possible to hide an advanced feature like field mapping from the user. In this case, field mapping remains in effect during synchronization, but is not accessible to the end-user. And lastly, it’s possible to make a component visible but read-only so as to prevent changes at the desktop. In short, the Configuration Manager unleashes the power to adapt both the user interface and functionality of deployed desktop applications.

The content of the user configuration is stored in a configuration file. Each configuration file corresponds to a mobile device, which means that several configuration files can be deployed on a desktop. And these configuration files can be deployed, managed, and changed remotely. This is further explained in the next section.

## Software Management

Once the license files and configuration files have been created, the Intellisync Desktop application is ready to be distributed. Enterprise Intellisync supports remote installation of the license, configuration and software files on the desktop computer. These can also be upgraded separately, which means that a change in the license or user configuration need not impact the desktop software itself.

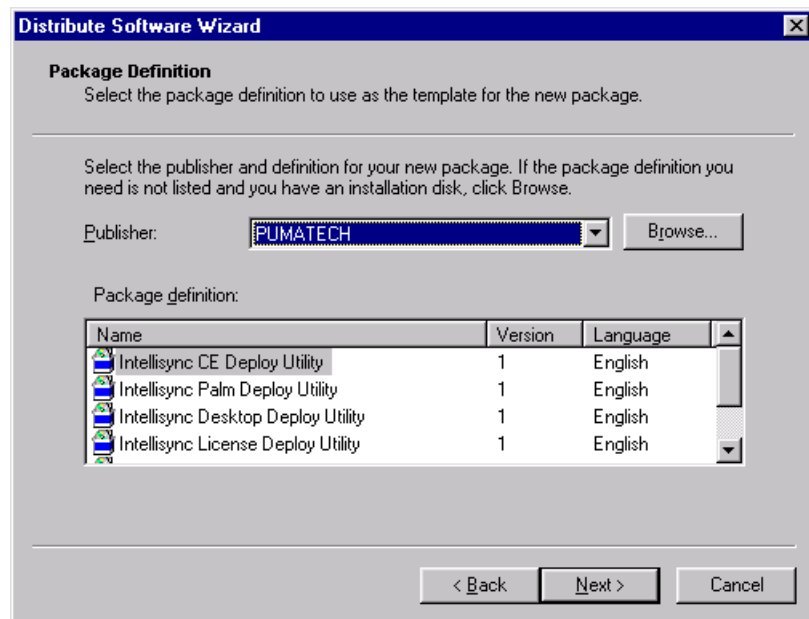
The Intellisync Desktop and associated files can be deployed using either Microsoft Systems Management Server (SMS), or a 3rd-party system management application available from companies like Tivoli, Novell and Computer Associates. Alternatively, the files can be manually distributed using Windows Explorer or standard email applications. Enterprise Intellisync automatically generates SMS package definition files that can be consumed directly by the SMS Administrator Console. This level of

*Enterprise Intellisync supports remote installation of the license, configuration, and software files on the desktop computer.*

*The Intellisync Desktop and associated files can be deployed using either Microsoft Systems Management Server (SMS), or a 3rd-party system management application.*

integration makes deployment of Intellisync Desktop effortless for enterprises already licensing SMS.

*Figure 7. SMS Screen with Intellisync Package Definition*



When installed as a standalone application, Intellisync Desktop requires user interaction to complete the installation and to create the user configuration. As with most desktop applications of this type, the user is typically prompted to enter the software key, and specify options such as the target installation directory, mobile device type, and desktop applications to synchronize (to mention a few). But Enterprise Intellisync supports a “silent install” mode, which eliminates the need for any user intervention at installation. By predefining all user settings in configuration files, the administrator can specify that installation involve no user input. The silent install mode is supported in conjunction with all installation methods (SMS and others). Enterprise Intellisync includes a special setup program that automatically applies the content of configurations to the desktops.

*Once installed, the Intellisync Desktop software can be upgraded remotely.*

Once installed, the Intellisync Desktop software can also be upgraded remotely. Whenever an upgrade is deployed, the administrator has the choice of preserving or overwriting the existing user configurations. This is especially useful if users are given the ability to modify default settings after installation. Users of Intellisync 3.5 or higher retain most settings, if so designated by the administrator. Preserved options include field mapping, conflict resolution, confirmation, date range, and filters. In summary, Enterprise Intellisync offers the following software management benefits:

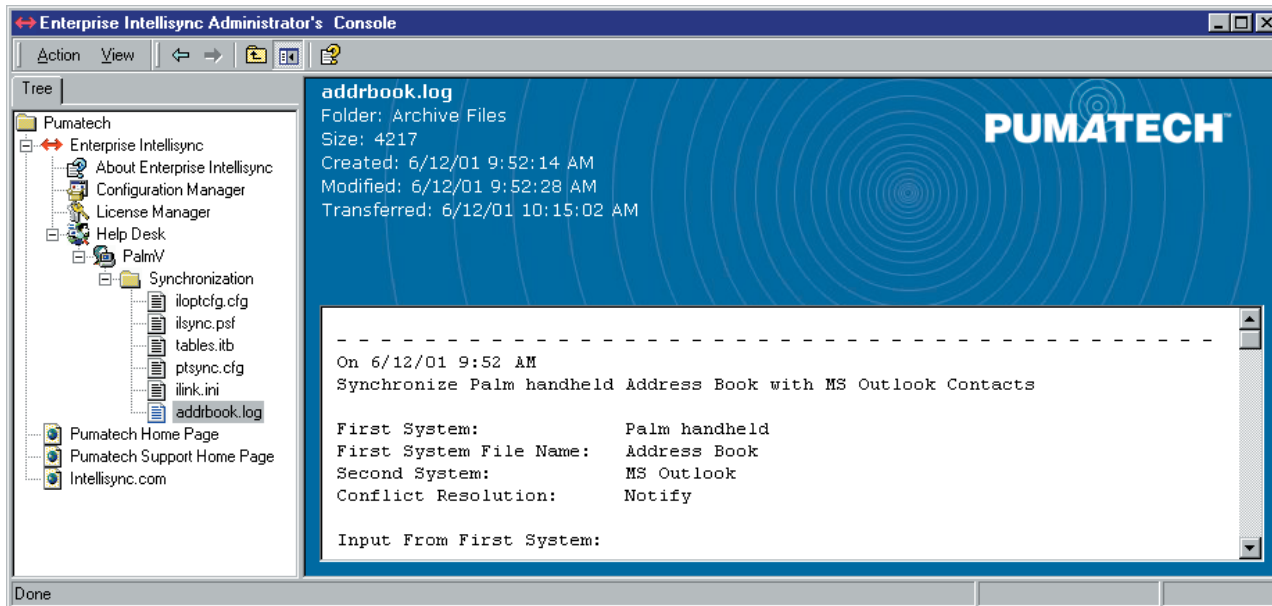
- \* Remote deployment of Intellisync Desktop and related files
- \* Close integration with Microsoft Systems Management Server (SMS)
- \* Flexible support for other software distribution mechanisms
- \* Silent installation to ensure bulletproof and friendly deployment
- \* Safe upgrades that preserve user configurations

### **Problem Management**

Centralized management goes a long way toward reducing the frequency of errors,

but cannot totally prevent them from occurring from time to time. The Enterprise Intellisync Help Desk is designed to speed up the analysis and resolution of problems wherever they arise. The Help Desk enables the administrator to receive, view, store, and forward details related to end-user problems in the field. These details are gathered in collaboration with Intellisync Desktop, which can create detailed logs of activities on demand. While Intellisync Desktop is responsible for logging detailed events, the Help Desk component provides the administrator tools necessary to analyze the content of these logs.

*The Help Desk enables the administrator to receive, view, store, and forward details related to end-user problems in the field.*



*Figure 8. Viewing end- user synchronization logs from the Administrator's Console*

The Help Desk component requires Microsoft Internet Information Server (IIS) to be installed on the Enterprise Intellisync server. A Pumatech extension to IIS must also be installed in order to enable sending and receiving of problem logs remotely. If necessary, the administrator can choose to enable logging only from select user configurations. And the Help Desk supports sending problem logs to any computer designated in each configuration. This means that it's possible to have logs forwarded to different computers depending on the user group originating the problem.

In keeping with Enterprise Intellisync's focus on simplicity, sending the logs involves a near-trivial action on the part of the user. From the Intellisync Support Tool on the Windows Start menu, the user simply selects the "Send All Logs" button. Also, the degree of details recorded can be changed using the Intellisync Support tool, but this is typically done with assistance from support personnel. Once received by the administrator, the user logs appear in the Administrator Console under the Help Desk. From here, the administrator can view and manage the logs. The Help Desk also provides a quick and easy mechanism for emailing log files to Pumatech for further analysis. In summary, the Help Desk offers these key benefits to the enterprise:

- \* Remote problem logs to speed up problem resolution
- \* Reduced number of troubleshooting visits to the desktop
- \* Simple user interface for end-users and administrators
- \* Extensive logging levels for more obtrusive problems



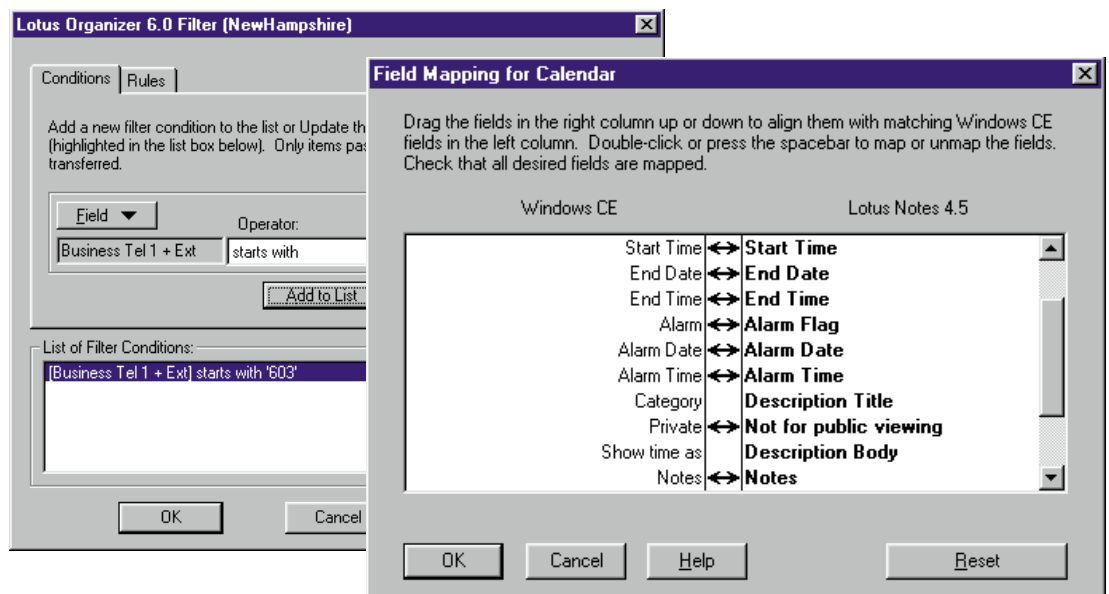
# The Enterprise Intellisync Desktop

*Intellisync Desktop is the most mature application in its category, having been in production since 1996.*

Intellisync Desktop is a central component in the Enterprise Intellisync suite of tools. This is by far the most visible piece, potentially deployed on numerous desktops spread across geographical locations. For this reason, it's crucial that the desktop application exhibit maturity and robustness to avoid costly support and usability problems. Intellisync Desktop is the most mature application in its category, having been in production since 1996. It's already the most-widely used synchronization application licensed in the enterprise environment. Not surprisingly, it has also won numerous recognition awards over its lifetime. In addition, Pumatech owns 9 patents in the area of synchronization, demonstrating clear leadership in its software category.

As the old expression goes, "the devil is in the details". And Pumatech has paid serious attention to all the important details required to support enterprise deployment. When teamed with the Administrator Console, Intellisync Desktop yields a bulletproof solution for desktop synchronization. To reduce downtime and user frustration, the application even builds in self-checking logic. For example, it automatically validates the license, configuration, and readiness of prerequisite applications every time it starts. This kind of meticulous attention to detail goes way beyond the simple sync functionality typically found in consumer applications. To further benefit the enterprise, Intellisync Desktop leverages de facto standards wherever possible. For example, it works with both Palm HotSync Manager and Microsoft ActiveSync to offer an integrated desktop solution.

*Figure 9. Filter and Field Mapping screens from Intellisync Desktop*



Intellisync Desktop is an integrated application, capable of supporting any number of mobile devices and applications from a single installation. It can be installed

either as a user-configurable or administrator-configurable application, to reflect the unique needs and policies of the enterprise customer. In addition, it leverages the Intellisync Connector technology in an effort to further protect enterprise investments in mobile software. Connectors are plug-in modules that can be deployed separately to support new devices and applications. These can be added over time with no impact on the core Intellisync Desktop software already installed on end-user systems.

Intellisync Desktop offers more features than any other product of its type. This is the culmination of years of experience, with more synchronization solutions deployed in the enterprise space than any other vendor. Its key features include:

*Intellisync Desktop offers more features than any other product of its type, with more synchronization solutions deployed in the enterprise space than any other vendor.*

a) **Field Mapping.** (See Figure 9) Field mapping specifies an association between data fields accessible in supported devices and applications. The mapping directs the flow of data among applications during synchronization operations. Intellisync Desktop automatically assigns default mappings between all common data fields, which are adequate for the majority of enterprises and users. But the enterprise can go further by adjusting the mapping of fields as needed to handle special cases. For example, most groupware applications support adding new fields. Intellisync Desktop provides the means for the administrator to synchronize these new fields through the field-mapping feature. End-users can also modify the mapping of fields on the desktop, but only if that privilege has been enabled by the administrator in the user configuration.

b) **Conflict Resolution.** Conflicts arise when the same data field has been changed differently in two or more applications. Note that Intellisync Desktop does not report a conflict if a field has been changed to the same value in multiple places, or if different fields were changed in various places. In the first case, Intellisync Desktop recognizes the duplicate change and simply ignores it without troubling the user with the obvious. In the second case, the application automatically merges the modified fields from the various sources to reflect combined changes everywhere. Intellisync Desktop uses the most advanced rules for detecting and resolving conflicts so as to ensure a simple and effortless user experience. Most notably, it performs synchronization at a field level rather than merely a record level. This means that only the affected fields are changed, leading to faster sync times. The finer level of sync granularity also serves to eliminate duplicate records, so often the bane of sync solutions. Intellisync Desktop applies superior conflict detection rules to deliver more accurate results and a more seamless user experience ("it just does it"). Several options are available to govern the handling of conflicts during synchronization. The administrator specifies the treatment of conflicts in the user configuration. Actions include adding new records to hold conflicting fields, ignoring incoming field conflicts, accepting only changes originating in one or the other application, and even prompting the user to choose visually among the conflicting fields.

c) **Filters.** (See Figure 9) When synchronizing data between a full-feature groupware application (like Microsoft Exchange) and a small mobile device

(like a Palm handheld), it's often necessary to limit the scope of data sent to the smaller device. In Intellisync Desktop, a "filter" is the primary mechanism used to control the data records transferred between applications. A filter consists of one or more field conditions, each of which contains a named field ("Category") from the application, an operator ("equals") and a field value ("Business"). Any number of field conditions can be combined to create a single filter, which is then applied during all succeeding sync operations. Intellisync Desktop provides the most powerful filtering capability of any application of its class. The administrator is able to predefine filters in user configurations to restrict the flow of data records. For example, the administrator can create and deploy a filter for the sales team that limits synchronized customer records to those falling within a geographic region. This can be done by configuring a filter condition such as "Region is Northeast".

d) **Confirmation.** To protect against unlikely but possible synchronization side effects, it's sometimes desirable to have the end-user verify the data changes before applying them. This gives users the comfort of knowing that no unexpected modifications are made to their data. Intellisync Desktop includes a unique feature that allows the user to see all changes before they're reflected in synchronized applications and devices. This option setting can be controlled by the administrator and deployed as part of the installed user configuration. When the option is set, a confirmation window appears during sync operations, showing the fields in each record that will be changed, if the user chooses to proceed. The option can be set to have all changes confirmed, or to record only deletions.

e) **Date and Task Range.** When synchronizing calendar applications, it's oftentimes appropriate to only transfer a subset of stored items. Similarly, when transferring task items, it's generally unnecessary to transfer those items already marked "completed" in the application. Specifying subset ranges tends to reduce both the time and storage required to synchronize with small mobile devices. Intellisync Desktop provides the options necessary to specify both the date range and task range of items. The administrator can enable only current and future calendar items to be transferred, or may choose to transfer all items dated a specified number of days before or after the current date. Likewise, to-do items can be restricted to synchronizing only those that are still "pending".

Intellisync Desktop is the leading synchronization application for mobile devices and enterprise groupware applications. The Administrator Console offers all the controls needed to safely harness the power of this mature application within the enterprise.





# About Pumatech

---

In the beginning, Pumatech was there. When mobile computing was in its infancy, we were already delivering real solutions. Even in the early days when “mobile computing” conjured up images of electronic organizers from companies like Sharp and Casio, we were there leading the charge. Since 1993, Pumatech has consistently delivered focused solutions for the mobile worker and the enterprise. As a data synchronization pioneer, we were also among the first to support true two-way sync with mobile devices. And we continue to be the leading supplier of sync solutions to this day, with experience that remains unsurpassed.

*Since 1993, Pumatech has consistently delivered focused solutions for the mobile worker and the enterprise.*

But sync is NOT everything. Over the years, Pumatech has developed, replaced, and acquired the technologies necessary to meet and even exceed the evolving needs of enterprises and partners. To that end, the breadth of our solutions has grown to embrace notebook computers (1993), handheld devices (1996), enterprise groupware applications (1999) and Internet services (2000). These advances were achieved quickly through the successful acquisition of eight technology companies, including several that specialize in Internet solutions. So, the new Pumatech combines the experience and technology of not just one but rather nine companies in total.

Leveraging its existing intellectual property, clear dominance in the sync space, and its newly acquired expertise, Pumatech is well positioned to future-proof your mobile investments against the chaos of a shifting market. Enterprise Intellisync provides a ready solution to the here-and-now problem of keeping your mobile solution under control.



# How to Contact Us

---

For More Information

## **On the Web**

[http://www.pumatech.com/enterprise\\_intellisync.html](http://www.pumatech.com/enterprise_intellisync.html)

## **Pumatech Headquarters**

2550 North First Street  
Suite #500  
San Jose Ca 95131  
Phone: 408-321-7650  
Fax: 408-321-3886

## **Corporate Sales**

Phone: 800-224-5430  
Fax: 408-321-3886

## **European Sales**

Phone

*United Kingdom, France, Germany, Ireland, Switzerland, Austria, Sweden, Norway,  
Netherlands, Denmark, Belgium*

Phone: 00800 78628324

*Finland*

Phone: 990800 78628324

*Spain*

Phone: 900 982922

*Italy*

Phone: 800 791311

Email: [europesales@pumatech.com](mailto:europesales@pumatech.com)

## **Asia Pacific Sales**

Phone: +612 9974 2739

Mobile: +614 03065842

Fax: +612 9974 2739

Email: [asiasales@pumatech.com](mailto:asiasales@pumatech.com)