

 **Ensure Technologies™**

User's Guide

XyLoc Client 9.x.x



© Ensure Technologies, 2009. All rights reserved

Table of Contents

Introduction.....	4
Your XyLoc Package	4
Support Information	4
XyLoc Core Functionality.....	5
XyLoc Solo Overview	6
The XyLoc System.....	6
XyLoc Product Architecture	7
How XyLoc Works	7
XyLoc Secure Login and Password Overview.....	8
Windows 2000/XP	8
Windows XP Embedded (XPe).....	8
XyLoc Password	9
Getting Started	11
Using the XyLoc Lock	11
Installing the XyLoc Lock (USB)	11
Placement of the XyLoc Lock.....	11
The XyLoc Lock Status Light.....	13
Using the XyLoc Key.....	14
Installing the XyLoc Software	16
Understanding Core Settings.....	28
Administrative Levels	28
Administrator	28
User	29
Guest	29
AutoLogon	29
Authentication Methods	29
Login Authentication.....	29
Unlock Authentication	30
Configuring the XyLoc Software	31
Security Configuration and User Preferences.....	31
User Setup.....	32
User Name.....	32
Add User	33
What It Does:	33
Delete User.....	33
Key ID.....	33
Add Key.....	33
Delete Key.....	33
Login Authentication.....	33
Allow Password Override (No Key)	34
Unlock Authentication	35
Allow Password Override (No Key)	35
Unlock to Key Only for up to <i>x</i> seconds/minutes	35
Range	36
Range Refinement	36
Personal Name	36
Advanced Settings.....	36
Advanced User Settings	37
Administrative Level.....	37
Auto Logoff Time	38
User can logoff locked workstation.....	38
Key ID.....	38
Lock Delay	39
Pass Key.....	39
Beep When Locking.....	39

Lock if the Key is Stationary for	40
XyLoc Password	40
What It Does:	40
Sets the XyLoc password	40
Note: This box will only appear if this key is part of a Kiosk Account.	40
Lock in Password Override	40
Run Application Integration Logoff	40
Setting the Active Zone	41
Adding New Users	43
Kiosk Accounts	46
Adding New Keys	47
PC Setup.....	49
XyLoc Lock Attached To.....	49
XyLoc Security Server	49
Log Records To Upload	50
Advanced Settings	50
Advanced PC Settings.....	51
XSS Client Port	51
Lock Delay	51
Min. Password Length.....	52
Logging	53
User Activity Log.....	53
NOTE: This option will only be available to a XyLoc Administrator.	53
Testing XyLoc Keys	54
Find Specific Key Mode.....	55
Find Strongest Key Mode.....	55
Sequence number	55
Range	56
Key Voltage	56
Key Revision.....	56
Overriding the XyLoc System.....	57
User Forgets Their Key.....	57
User Does Not Have a XyLoc Key.....	58
Unlocking using Password Override.....	58
Using Microsoft Remote Desktop Protocol (RDP).....	58
Replacing the XyLoc Battery	59
Software Removal.....	59
Troubleshooting	60
System Functionality	61
Normal Operational Mode	61
Hardware Architecture	61
Radio Frequency (RF) System	61
Spectral Reuse.....	62
Time Division Multiple Access (TDMA)	62
Technical Specifications	62
Revision History	63

© Ensure Technologies, 1998-2008. All rights reserved. XyLoc and Ensure Technologies are trademarks of Ensure Technologies, Inc. Other trademarks are the property of their respective owners.

Acrobat® Reader copyright © 1987-2008 Adobe Systems Incorporated. All rights reserved. Adobe and Acrobat are trademarks of Adobe Systems Incorporated

Technical information contained herein is subject to change without notice.

Introduction

Your XyLoc Package

The following is a checklist of all items included in the XyLoc User's Package:

- ❑ Quick Start Instructions
- ❑ XyLoc Solo
 - XyLoc Key
 - XyLoc USB Lock
 - USB Extension Cable
 - XyLoc Lanyard
- ❑ CD-ROM containing:
 - XyLoc software installer
 - Software Release Notes
 - Electronic version of XyLoc User's Guide in Adobe Acrobat format
 - Adobe Acrobat Reader installer

Support Information

We are available to answer any questions or provide any needed assistance. Please contact:

Ensure Technologies
Technical Support
(734) 547-1631

support@ensuretech.com

FCC Compliance

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation of this device is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications not expressly approved by Ensure Technologies for compliance could void the user's authority to operate the equipment. The term "IC:" before the radio certification number only signifies that Industry Canada technical specifications were met.

XyLoc Core Functionality

The XyLoc Solo is a flexible hardware/software platform with expanding capabilities. Below is an overview of the core capabilities in the XyLoc Solo and future capabilities.

<i>Capability</i>	<i>Functionality</i>
Full-Time Access Control	Continuously monitors for the presence or absence of authorized users, secures the PC when user leaves Active Zone , and unlocks when user returns
Proximity-Based ID and Authentication	Confirms the user's identity and verifies authorized access to the PC based on user's proximity to PC
Automatic Network Logon	Provides automatic logon to pre-configured network services; maintains network sessions when the user leaves Active Zone .
Multi-User Support	One Key can be programmed to unlock hundreds of Locks (for system administrators or department managers); One Lock can support multiple Keys (for shared PC environments); Kiosk accounts
Access Methods	<i>Single factor security:</i> Hands-Free, Select User Name <i>Dual factor security (recommended):</i> Must Enter Password
Transparent Operation	Protects PC without requiring any action or intervention by the user
Programmable Range	User-definable Active Zone for maximum flexibility
Management	User or administrator locally manages and administers XyLoc system
System Connection	Connects via the USB port
OS Support	Windows 2000, and XP. NOTE: Windows 95, Windows 98, NT4 and Windows ME are not supported
Key Type	KeyCard
Installation	Installs in minutes using only one cable and simple installation Wizard
Screen Saver Support	Any windows screen saver is supported. NOTE: Since XyLoc takes over the security of the workstation a password protected screen saver in Windows 2000/XP is no longer available or needed. XyLoc will secure the workstation for the user immediately when they exit the Active Zone.
Scalable Management	XyLoc Security Server for central management and audit log tracking of the users

XyLoc Solo Overview

XyLoc Solo delivers desktop security that positively identifies authorized users and permits access to PCs and portables as appropriate.

The focus of XyLoc Solo is three-fold:

1. Providing full-time access control to PCs and portables
2. Taking the burden of compliance off the end user
3. Making the computer more convenient for the user

XyLoc Solo runs on Windows 2000 and Windows XP. It has been designed with careful consideration to the varying security dynamics of these operating systems. XyLoc provides an additional layer of protection to the built-in security capabilities of Windows 2000 and XP.

The XyLoc System

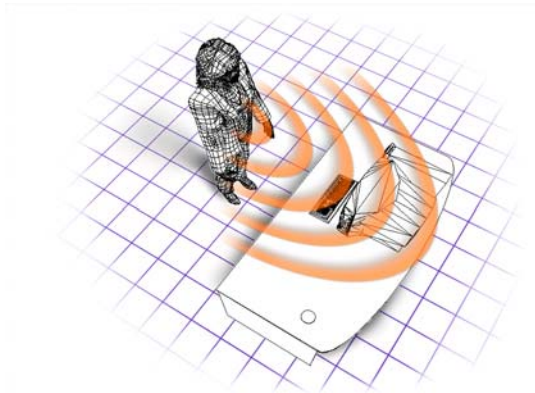


XyLoc Product Architecture

XyLoc is a microprocessor-based turnkey solution. Its patented technology is based on wireless radio frequency (RF) technology that continuously monitors authorized users based on their proximity to the PC and grants access to the PC as appropriate. The XyLoc system consists of:

- **XyLoc Software:** authenticates and identifies multiple users and controls the lock and key;
- **XyLoc Lock:** a small ultra-low power receiver that plugs into a USB port;
- **XyLoc Key:** a small, wireless transmitter with unique user ID that can be clipped to a belt or key ring, worn on a neck lanyard, or attached to an ID badge.

How XyLoc Works



The XyLoc Lock and Key are in constant, encoded two-way wireless communication with each other. As an authorized user approaches the PC, the XyLoc Key identifies and authenticates the user, and unlocks the PC when the user enters the pre-set **Range**. Then, when the authorized user moves out of the **Active Zone**, XyLoc automatically secures the desktop. The PC is instantly secured and remains so until an authorized user returns to within a user-configured unlock range. Background tasks, such as printing and downloading, however, may continue while the PC is securely locked.

XyLoc Secure Login and Password Overview

Windows 2000/XP

The Windows NT based Operating Systems (2000/XP) are designed with inherent security. There is already a GINA in place which controls the logins, profiles and security permissions on the workstation. The XyLoc system also has a GINA, which takes over the primary windows logon and in turn “calls” the Microsoft GINA. Most of the inherent Microsoft security is still in place, and XyLoc enhances that security with a proximity based solution.

The XyLoc Secure Login will be the first screen that is displayed on the PC, and the same basic login process will be used. The exception is that hitting “CTRL+ALT+DEL” on the keyboard will allow access to the standard Microsoft/Novell login box and a user can login with a valid local or domain account and override XyLoc. This is to allow an Administrator to still gain access to the PC, even if that Administrator does not have a XyLoc account. There is a registry setting that can be enabled which will block all non-XyLoc accounts from gaining access to the system, even Administrators, however this setting is disabled on the default installation.

Also, the F8 keystroke at boot up is not disabled at login. This is due to the security of Windows itself, and only an Administrator should have access to truly bypass XyLoc in Safe Mode.

Lastly, in Windows 2000/XP, the password-protected screensaver is no longer password protected. Because XyLoc takes control of the security of the workstation, XyLoc also handles the locking action of the PC. Since the system will lock immediately when the user leaves his/her active range the password protection on the screensaver is no longer needed. It will still function as a standard screensaver, but will no longer have a password.

Windows XP Embedded (XPe)

Windows XP Embedded (XPe) is a scaled down version of the Windows XP Professional Operating System. Original Equipment Manufacturers (OEMs) can decide which elements are needed or not when designing their thin clients, allowing for streamlining the hardware needed.

Each manufacturer’s build is different. It is important to understand the customized XPe operating system utilities and security feature of a particular device when installing software.

Most XPe operating will revert to their original conditions upon reboot unless necessary configurations occur, e.g. setting the ‘Write Filter’; utilities to ignore certain files and/or processes.

Here are items to remember when installing the XyLoc Client on Windows XPe:

- You must be logged into the thin client with the built in ‘Administrator’ account to install the XyLoc software.

- When installing on the Windows XPe Operating System, XyLoc Client only supports English. The other language versions have been removed to keep the install package as small enough to be able to be installed on a Windows XPe thin client device.
- When the installation finishes, do not select the option to restart automatically. Select the option to restart manually later. After the installation, the internal cache must be “flushed” using the built in “Write Filter” utility of the manufacturer’s particular XPe build. This will take the changes that were made and write them to the internal flash memory. If this process is not done, any changes made will be lost on the next reboot of the device.
 - NOTE: In some XPe devices, logging in as the built-in Administrator account turns off the “Write Filter” automatically. If this is the case, then there is no need to flush the cache to permanently write the changes. Please consult with your device documentation for more information on that functionality.
- If the XPe build has the capability to have the Write Filter ‘ignore’ selected Windows files and/or processes after a reboot, please select the following:
 - Files:
 - C:\%WIN_DIR%\System32\XyLocUF2.LBE
 - C:\%WIN_DIR%\System32\XyLocMF2.LBE
 - Processes:
 - xyloc.exe
 - xylocicon.exe
 - xylocait.exe

XyLoc Password

For flexibility and security, the XyLoc system provides an additional password, the **XyLoc Password** (sometimes referred to as a PIN). The XyLoc password is only used in a Kiosk account and has two possible applications:

1. It is used by the **Kiosk Account** feature to provide multi-factor authentication in a shared log-on account. **NOTE:** Starting in version 8.2.4, this is the only password that is accepted in conjunction with a user’s XyLoc key.
2. It is used in conjunction with the user’s **Personal Name** when performing a **Password Override** in a Kiosk account to ensure individual security even when a XyLoc Key is not present.

NOTE: In a XyLoc Solo, when used in a unique account environment, the XyLoc Password (PIN) will synchronize with the user’s unique account password. The Kiosk account is the only type that will have a XyLoc password that can differ from the user’s system account

password. If it is desired to use at PIN with a unique account, XyLoc 8.3.6 **with** XSS 4.2.4 must be used. Earlier version of either will not support this functionality.

Getting Started

Using the XyLoc Lock

The XyLoc Lock included in this package is a low power receiver that is connected to the PC through a USB interface.

Note: Windows 2000/XP/XPe users must have *local* Administrator privileges to complete the installation.

Installing the XyLoc Lock (USB)

1. Close all open applications.
2. **Please wait to attach USB XyLoc lock until prompted by XyLoc software install wizard.**
3. Insert the XyLoc CD into the CD drive.
4. Install the **XyLoc System Software**. Locate the latest installation file (EXE) in the 'XyLoc Client Software'. Double-click the file to start the installation and follow the instructions.



USB Plug

Placement of the XyLoc Lock

XyLoc uses advanced wireless technology to make PC security more convenient for the user. The proper placement of the XyLoc Lock will ensure that users get the best performance from XyLoc. For additional guidelines and suggestions, please view the “**Using XyLoc End User**” or “**XyLoc Orientation Guide**” included on the installation CD.

Ideal placement is with the face of the Key parallel to the LED on the front of the Lock. The best performance of the system will be achieved by trying to maintain this positioning while you are seated at your PC doing your work.

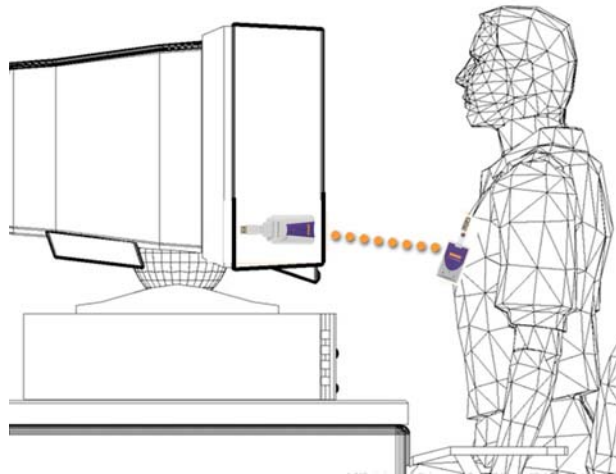
The primary factor in deciding where to place the XyLoc Lock is to determine where the user will wear the XyLoc Key the majority of the time. The Key can be clipped to a shirt pocket or belt or worn on a lanyard around the user’s neck.

Once you’ve identified where the Key will be worn, place the Lock at the same height as where the Key will be when the user is at the PC. You should also make sure that the path between the Lock and Key is unobstructed (such as obstruction caused by your arm that might occur while using your mouse or keyboard).

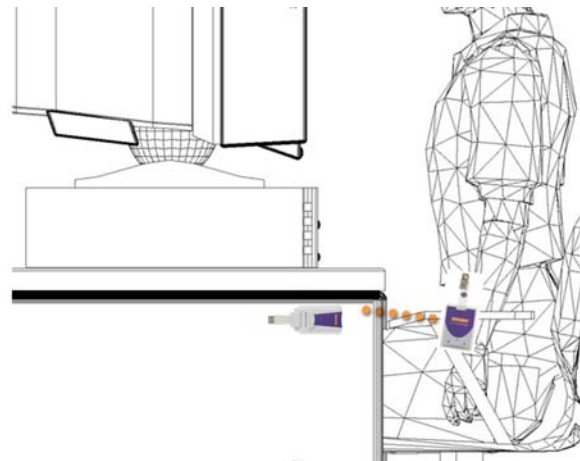
For example, if the user will wear the Key on the left side of the shirt, use the Velcro strip to secure the Lock to the left side of the user's monitor at the same height as the Key will be when the user is seated.

If the user will wear the Key on the right side of the belt, use the Velcro strip to secure the Lock to the underside of the user's desk. The Lock should be at the same height as the Key will be when the user is seated. The user should keep the face of the Key pointing at the LED.

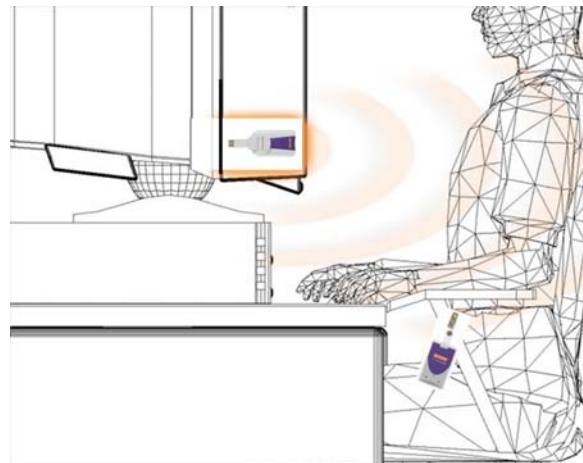
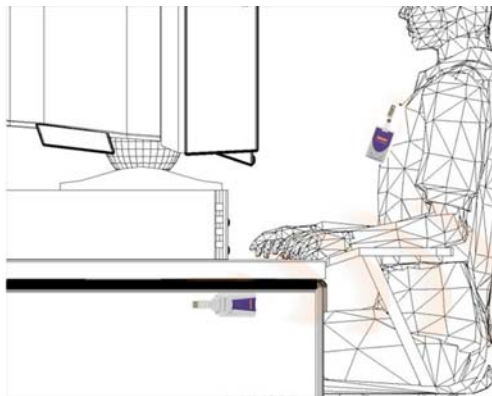
Ideal Lock Placement



Acceptable Lock Placement



Less Desirable Lock Placement



The XyLoc Lock Status Light

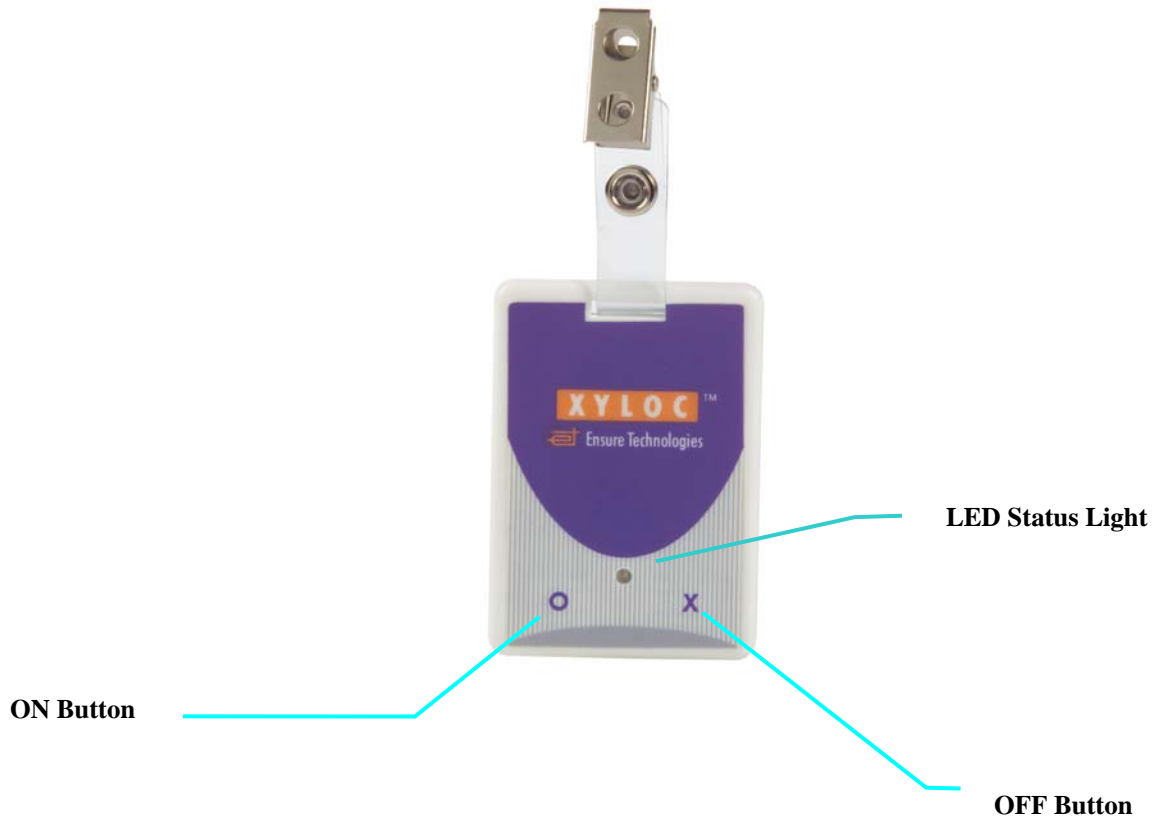
The LED indicator light on the XyLoc Lock has four possible states:

1. **Green** – The indicator light is **green** when the computer is unlocked and available for access.
2. **Red** – The indicator light is **red** when the computer is locked or disabled.
3. **Orange** – The indicator light is **orange** when the computer is running the ‘Lock Delay’ timer.
4. **[Off]** – The indicator light is **off** if the XyLoc system is not receiving power.



Using the XyLoc Key

The XyLoc Key is a low power radio transmitter with a unique non-volatile user identification code that cannot be cloned.



The **KeyCard** is powered by single coin cell that last approximately twelve to twenty-four months. The **KeyCard** has two switches on its front panel marked “O” and “X”. The “O” turns the **Key ON** and “X” manually turns the **Key OFF**. The **Status LED** flashes green when the system is turned **ON** and red when it is turned **OFF**. The **OFF** action requires an extended depression of the “X” button to turn the **Key OFF**, but to turn the key **ON** just press and release the “O” button.

The **KeyCard** uses sophisticated power management technology and will automatically turn **OFF** approximately 13.5 hours after it was first turned **ON**. You may extend this automatic turn **OFF** time up to 3 additional hours by pressing the “O” button one time for each additional hour, any time after the **Key** has been turned **ON**.

The **Status LED** also functions as a battery tester. As long as the **LED** functions, the **KeyCard** has sufficient battery power. The XyLoc software also incorporates a **Battery Voltage Meter** with which the user may check the battery life through the XyLoc configuration software (See the section for **Testing the XyLoc Keys**). Also, the XyLoc Security Server (XSS) at any time has a status log that reports when a battery is running low on battery life. Please review the XSS User Guide for more details.

The **Key** must be in the possession of the user at all times. The XyLoc system provides tools to help ensure user compliance. XyLoc is capable of identifying a **Key** that has been left stationary. The XyLoc system can be configured to automatically secure the workstation, should a **Key** be left unattended. This action is also recorded in the Audit Logs.

NOTE: To insert the battery into the KeyCard, place the KeyCard with the XyLoc logo face down, remove the two retaining screws and slide open the lid. Replace the CR 3032 coin cell with the “+” up.

Installing the XyLoc Software

The XyLoc software controls the operation of the Lock/Key and their interaction with the PC's operating system. The software offers flexible configuration options and selectable desktop preferences to meet the users varying needs. Installation is accomplished via a simple-to-use wizard.

Except where noted, the following instructions apply to all supported Microsoft Windows systems.

NOTE: Windows 2000/XP users must have *local* Administrator privileges to complete the installation.

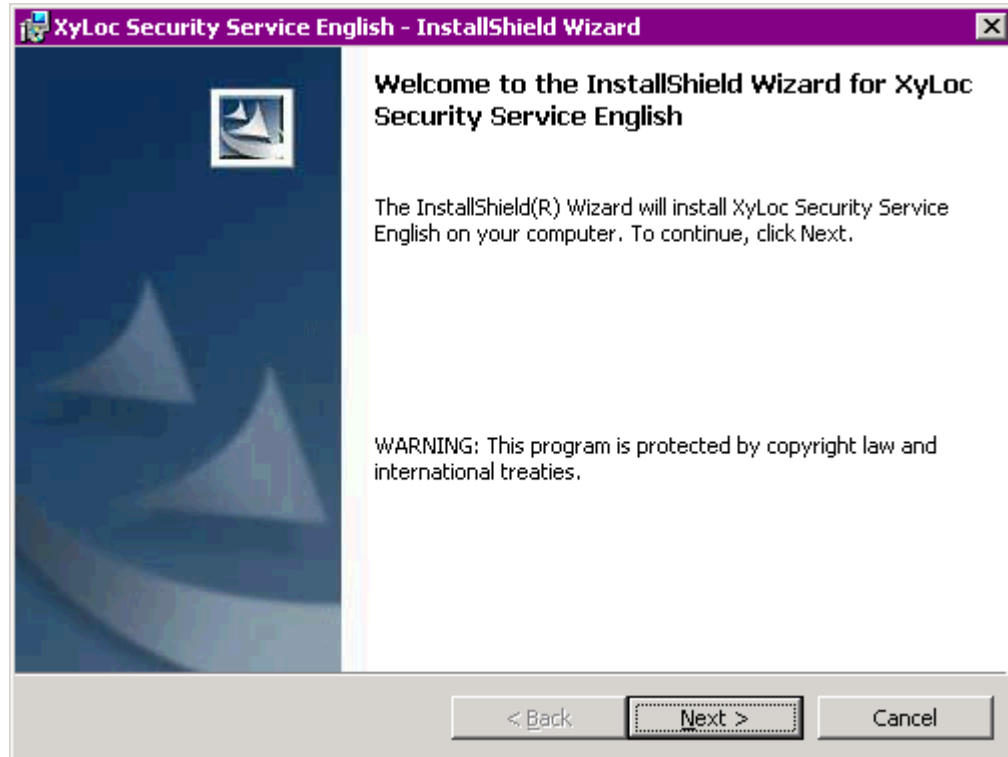
NOTE: When installed on Windows XPe, the XyLoc client only supports English. The other language versions have been removed to keep the install package small enough to be installed on a Windows XPe Thin Client device.

NOTE: In version 8.2.4 the installation program was changed to an MSI based installer. This has changed some of the installation process slightly as well as the screens that are displayed. The instructions below are for this new installer, except where indicated.

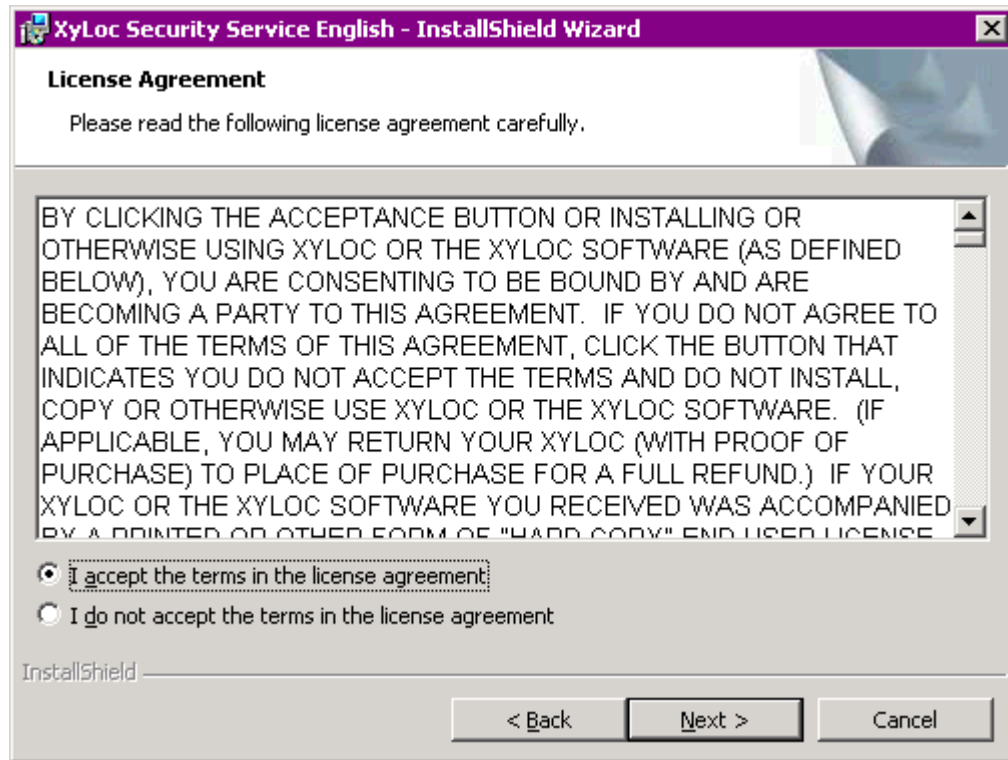
1. Exit any applications that are currently running.
2. Place the XyLoc CD-ROM into the CD-ROM drive. .
3. Use either My Computer or Windows Explorer to select the CD-ROM drive, and locate the latest installation file (EXE) in the 'XyLoc Client Software' folder. Double-click the file to launch and then follow the Wizard's instructions.
4. Select the language for the installation.



5. Click **Next** on the welcome screen to continue with installation.

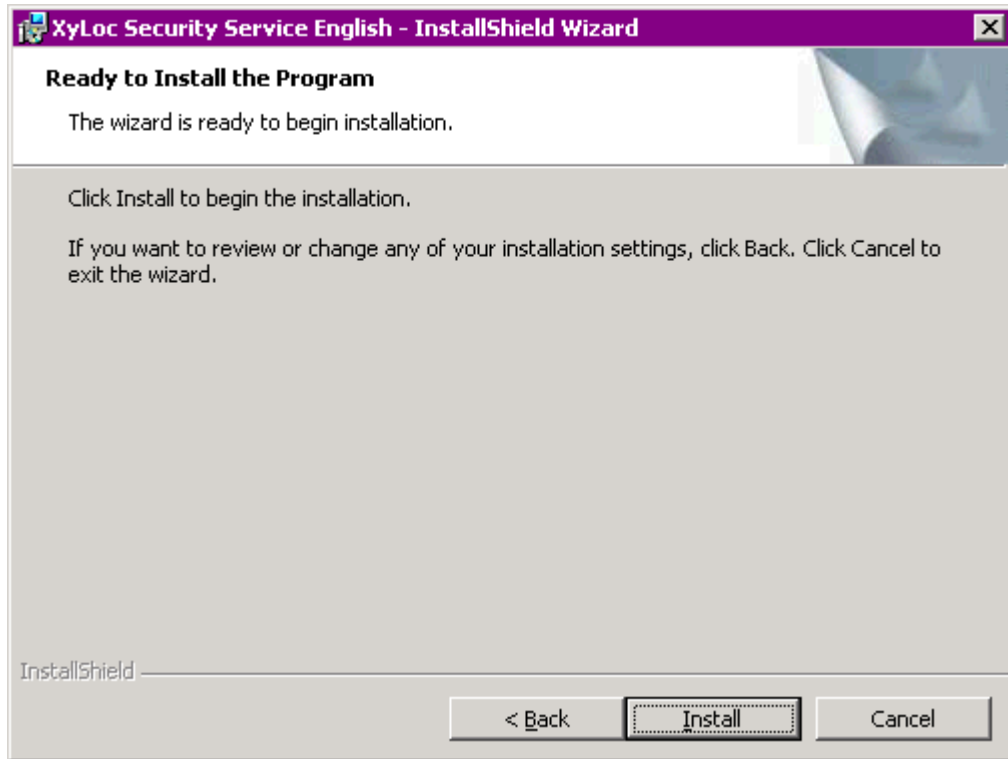


6. Please review the terms of the **Software License Agreement**. If you accept all of the terms of the Software License Agreement, click **Yes**, and the installation will continue. If you do not accept all of the terms of the Software License Agreement, click **No** to cancel the installation process.

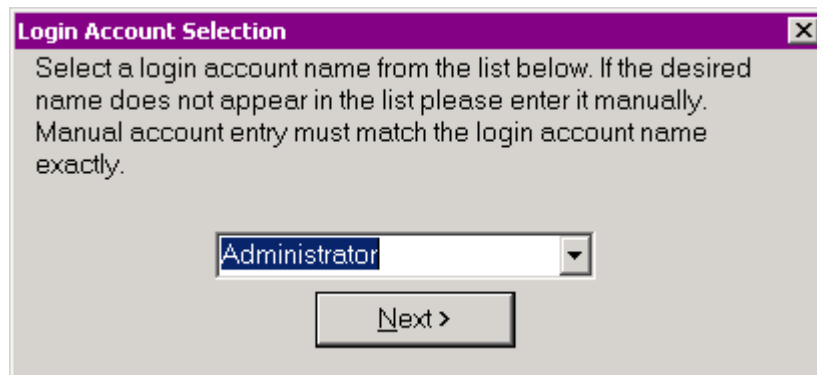


7. Once the program is ready to install the files, the “Ready to Install” window will display. Click “Install” on this screen when you are ready to install

NOTE: This screen does not come up in 8.2.3 and earlier)

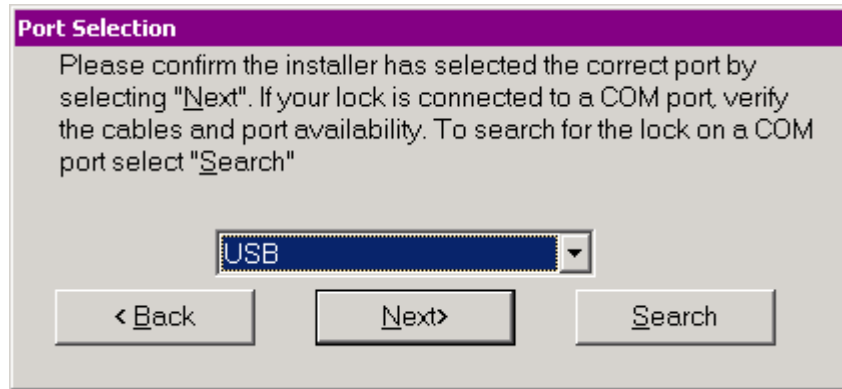


8. **Login Account Selection:** Select the desired user name from the list. This list is created by examining the Users database on the PC. If XyLoc is to be configured for a network logon account, type the account name here, being careful to enter the name exactly as it appears for your normal logon. Please create a user via the **Users** control panel in Windows.



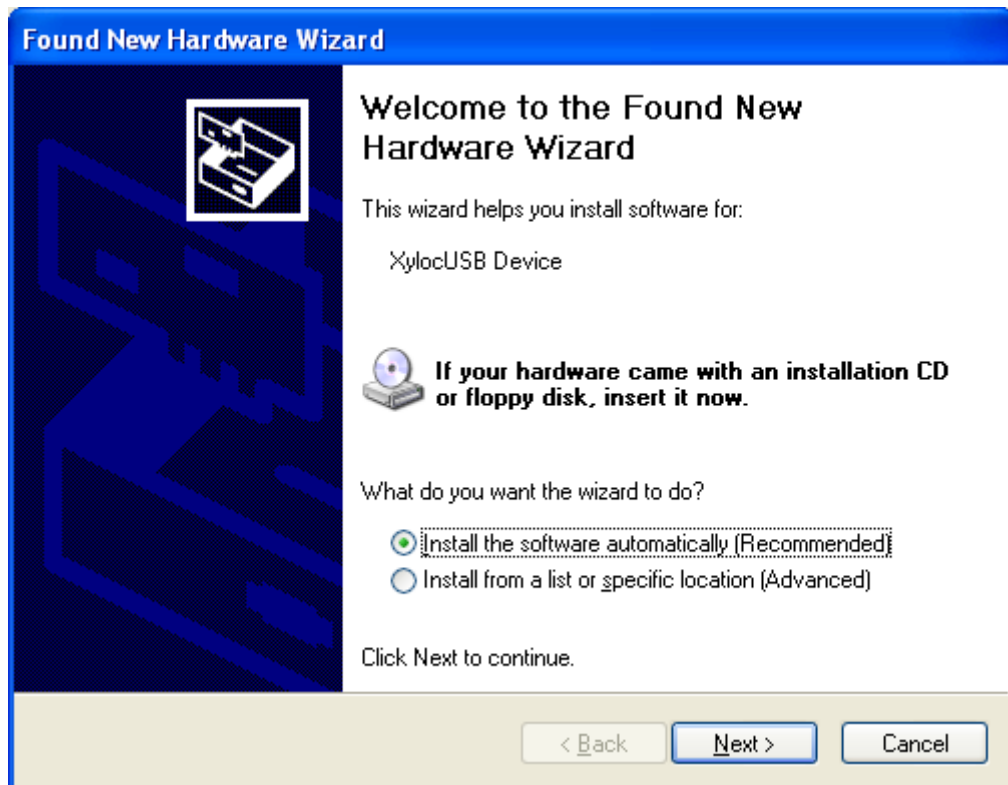
9. **Lock Identification:** XyLoc will attempt to find the port to which the Lock is attached. Click OK to continue. On a new installation, the Lock should not be connected yet,

therefore XyLoc will not find the Lock. The **Port Selection** screen will appear. Please confirm that the correct port has been selected and correct it if necessary. Click “Next”.

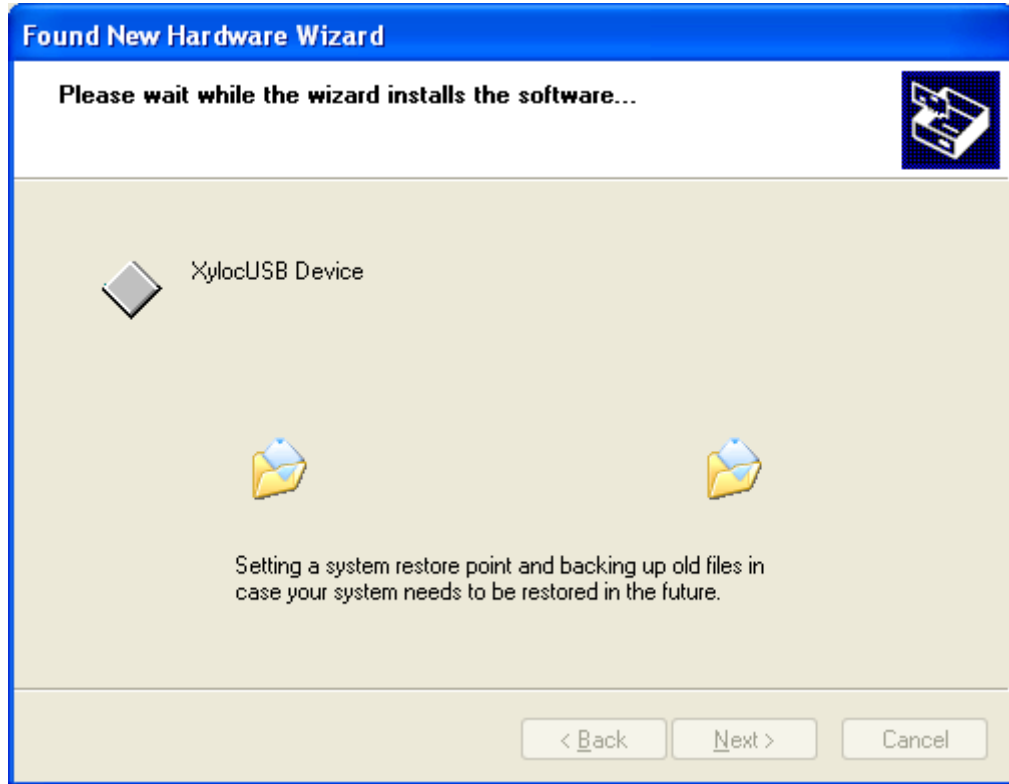


10. If you are using the USB version, connect the lock to the computer at this time.

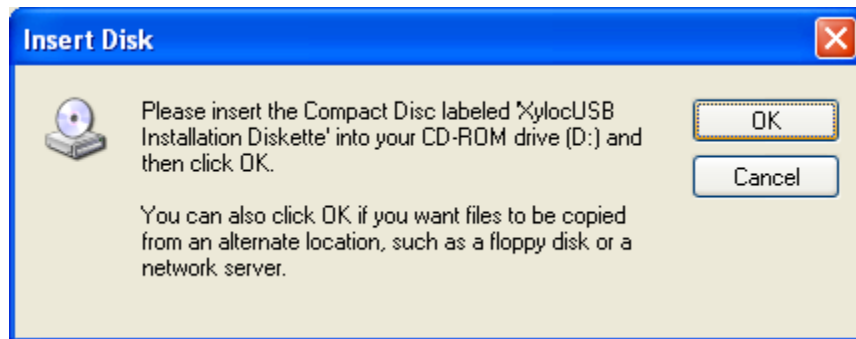
NOTE: On Windows XP, the Found New Hardware Wizard will appear. Leave the default for “Install the software automatically (Recommended)” and click Next.

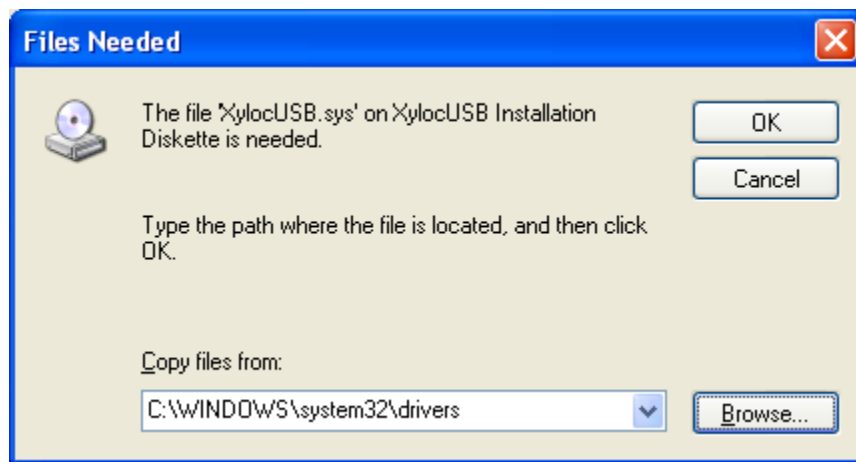


11. Let the system find the drivers and install automatically.



12. If for some reason Windows XP does not find the driver it will likely prompt the user to “Insert the disk labeled XyLocUSB Installation Diskette.” If this occurs, click **OK**, and then click **Browse**. Point to “C:\WINDOWS\System32\Drivers\” directory, which should contain the XyLocUSB.sys file necessary to install the USB device. Click **OK**.





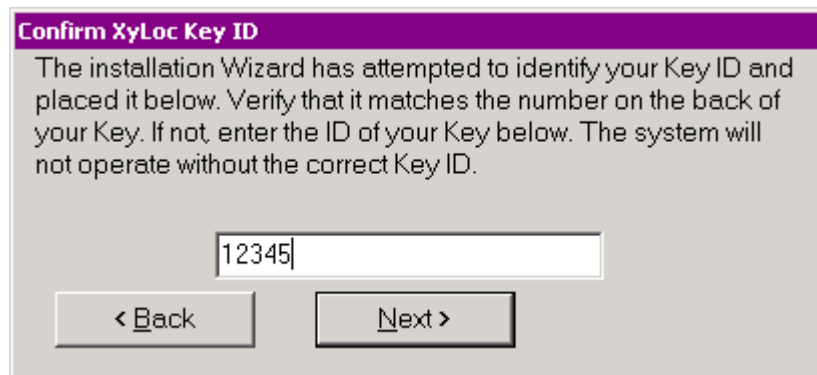
13. Click "Finish" to complete the new device installation.



14. Once Windows has finished installing the device, click “Continue.”

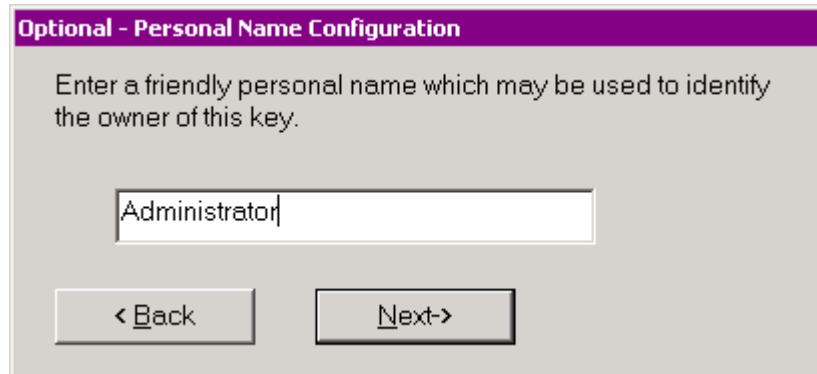


15. **Confirm XyLoc Key ID:** XyLoc will attempt to identify the closest Key and insert that Key ID into this field. Refer to the label on your XyLoc Key and verify that it matches the Key ID shown. If no Key ID is shown, or if it is not the correct Key ID, please enter it manually.



16. **Personal Name Identification:** Enter the user's full name to further identify the Key owner.

NOTE: This field is an optional field. If the name is left blank, the actual Account Name will be used instead.



Optional - Personal Name Configuration

Enter a friendly personal name which may be used to identify the owner of this key.

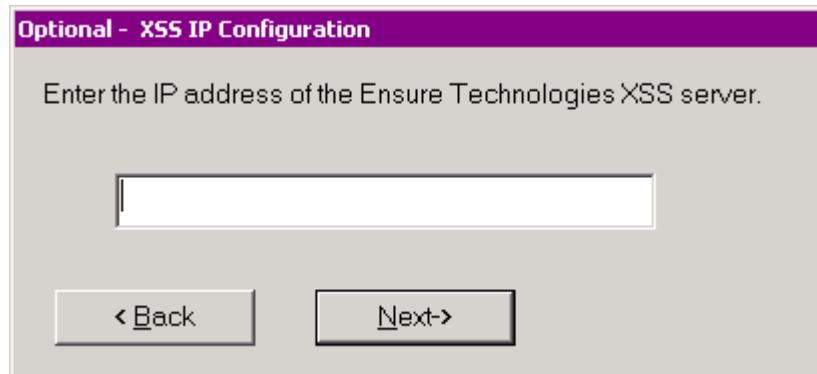
Administrator

< Back Next->

17. **XSS IP Configuration.** This screen has a field to enter the address of the XSS (XyLoc Security Server), if there is one.

If there is no XSS, this field can be left blank.

NOTE: XyLoc 8.2.4 also added the ability to use the server's DNS name for the address instead of the IP address. You can enter either address at this screen.

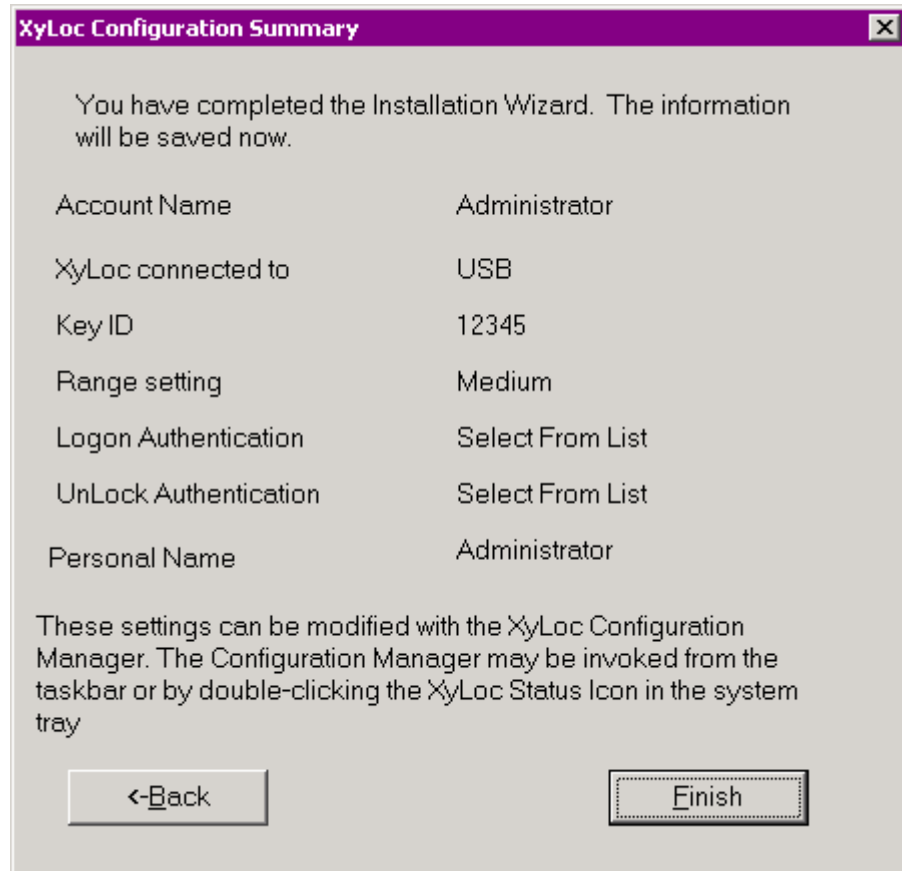


Optional - XSS IP Configuration

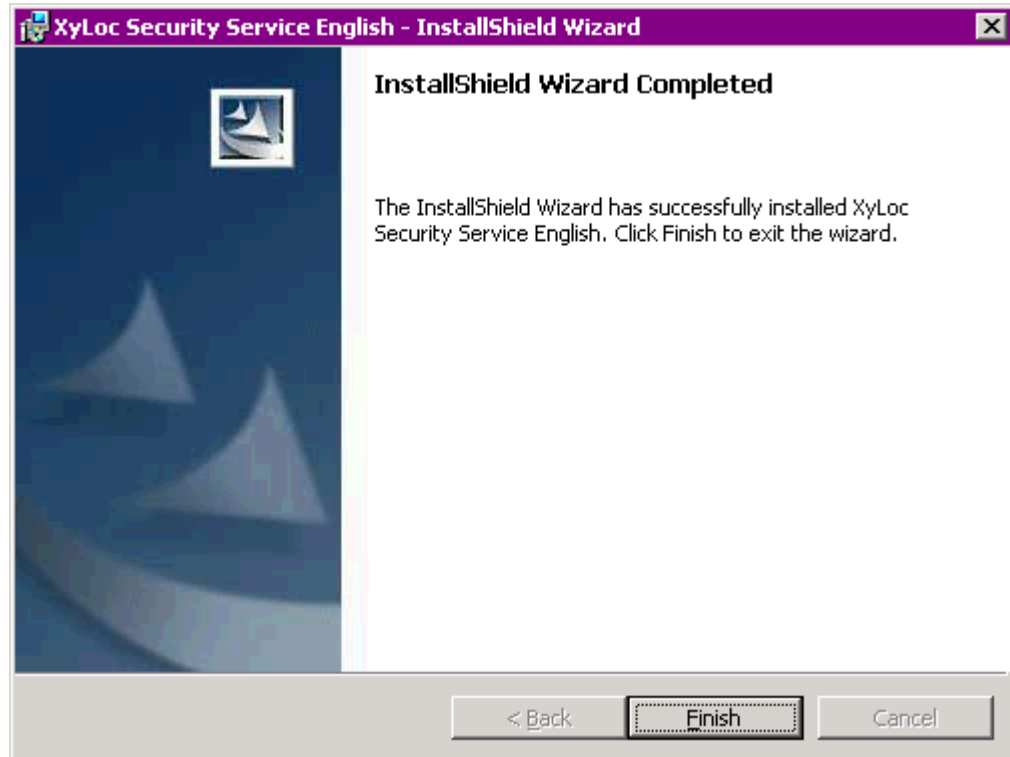
Enter the IP address of the Ensure Technologies XSS server.

< Back Next->

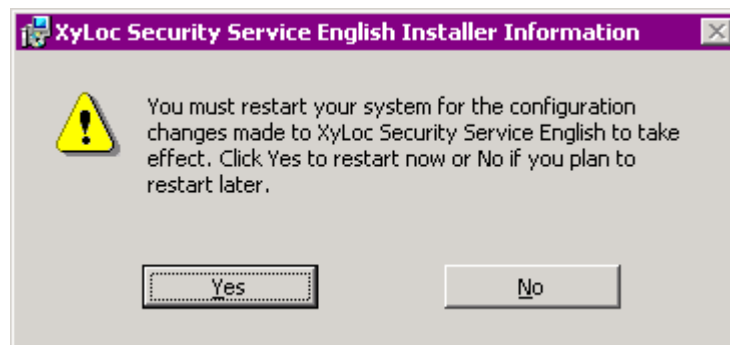
18. **XyLoc Configuration Summary.** This screen provides a summary of the features you just selected. Choose **Finish** to complete the **Installation Wizard**.



19. Click “Finish” once the installation is complete.



20. Restart your computer when prompted.



21. If your installation was successful, upon restart you will see the XyLoc logon window. Logon by clicking on the personal name associated with the XyLoc key.
22. Your network provider logon screen (Microsoft or Novell) will then appear. Enter your system account password. Unless your system account password periodically expires, this will be the last time you will be asked to enter your Microsoft or Novell password from the network provider logon screen.
23. Once the desktop appears you will also see a XyLoc Status message that will appear briefly in the system tray. By default, this message will appear whenever the XyLoc Status changes (unlocking, disabled, etc.). NOTE: If it is desired to have this status

message appear at all times, then right-click on the XyLoc icon and click on “Show XyLoc State.” This will cause the XyLoc Status window to stay resident on the desktop.



24. The XyLoc icon should also be displayed in your system tray.



25. Test your XyLoc system by stepping away from your PC and watch to see if it secures. If it does, you’re all set and ready to go! You can also adjust the range at which the XyLoc locks and unlocks your PC – see **Setting the Active Zone** in the section for **Advanced User Settings**.
26. To further customize your installation, follow the directions under **Configuring the XyLoc Software**.

NOTE: The XyLoc icon in the System Tray can be used to view the status of your system and to help troubleshoot the system. Simply move your cursor over the XyLoc icon to view the pop-up that will provide the status of the system.

Understanding Core Settings

Although a detailed description of the many XyLoc configuration options is discussed in the **Configuring the XyLoc Software** section, an overview of the differences among the core settings is useful.

Administrative Levels

All authorized XyLoc Keys will grant a person access to a particular PC. However, there are three different **Administrative Levels** that affect that person's ability to make changes to the way XyLoc operates.

The **Administrative Levels** are set under the **Advanced Settings** button in the **User Setup** tab of the **XyLoc Configuration Manager** (see **Getting Started – User Setup**). Only an **Administrator** can access the **Administrative Levels** settings:

	User Setup	PC Setup
Administrator	<i>Full access to Configuration Manager and all Users' settings</i>	
User*	Only Range Settings and Personal Name can be changed	<i>No changes can be made</i>
Guest	<i>No access to XyLoc Configuration Manager</i>	

* A **User** can only access his/her own settings: no one else's settings will be visible or accessible

Administrator

A person with **Administrator** privileges has complete access to all of the features of the **XyLoc Configuration Manager**. This includes the ability to add and delete users from the database and to create and modify all settings for individual users.

NOTE: Each XyLoc installation must have at least one user with **Administrator** privileges.

The **Administrator** level is appropriate for the person with the responsibility of managing an organization's security or IT infrastructure.

User

A person with **User** privileges has limited access to the features of the **XyLoc Configuration Manager**. This level is best suited for most users. These users need regular access to a particular PC and would benefit from the ability to modify the way XyLoc works in their specific environment.

A person with **User** privileges will only see their name in the **User Name** field – no other people's names will be visible or accessible.

The only settings available for modification under the **User Setup** tab are **Range**, **Range Refinement** and **Personal Name**.

Guest

A person with **Guest** privileges will not be able to launch the **XyLoc Configuration Manager**. This level is helpful even for regular users to prevent a user from accidentally leaving the Configuration Manager open and disabling the XyLoc security.

AutoLogon

XyLoc's AutoLogon feature simplifies the logon process for the user. The first time a user successfully logs in to XyLoc (using any of the methods described below) they will be prompted to enter their network logon and password. The next time the user logs in XyLoc will automatically log the user in to their network account.

Authentication Methods

There are two types of authentication settings available in the **User Setup** tab of the **XyLoc Configuration Manger: Login Authentication** and **Unlock Authentication** (see **User Setup**). The **Login Authentication** setting determines the method of authentication during login, and the **Unlock Authentication** setting determines the method of authentication once a user has logged in and XyLoc locks the PC. Your choice of settings will likely be driven by your organization's security policies and your specific security needs:

Login Authentication

- **Hands-Free AutoLogon:** This setting provides the most convenience. When an authorized user enters the **Active Zone**, the user is automatically logged in without requiring that any other action be taken.
- **Select User Name:** This setting finds all the keys in the area and then prompts the user to select their name from the list of users found.

- **Must Enter Password:** This setting requires that a user enter his/her password before that user is logged in. The system will display all the authorized keys in the area and once the user selects their name from the list, they will be prompted for their password. If only one user is found, the system will display the password prompt automatically.

Unlock Authentication

- **Hands-Free Unlock:** This setting provides the most convenience. When an authorized user enters the **Active Zone**, the PC is automatically unlocked without requiring that any other action be taken.
- **Select User Name:** This setting finds all the keys in the area and then prompts the user to select their name from the list of users found.
- **Must Enter Password:** This setting requires that a user enter his/her password before that user can unlock. The system will display all the authorized keys in the area and once the user selects their name from the list, they will be prompted for their password. At Unlock, the user must select their name from the list regardless of how many keys are found. Unlike at Login, the password prompt will **not** be displayed automatically.

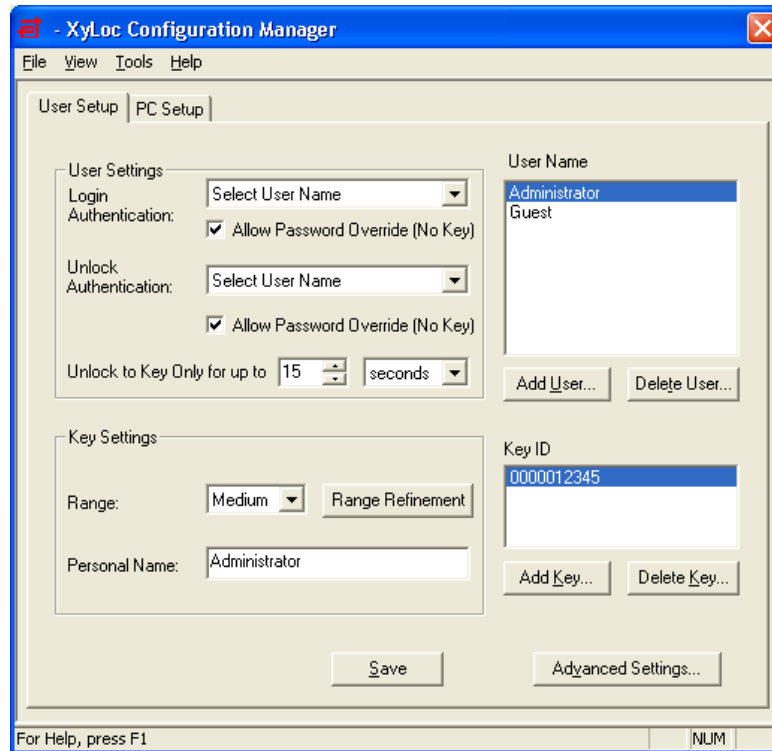
Administrators should also see the Allow Password Override (No Key) option under the User Setup section for information on requiring both a password and a key to unlock a computer.

Note: If there is only one administrative account on the PC, that Administrator may not disable **Allow Password Override** for himself. At least one administrator on every machine must be allowed to password override as a safety precaution. Thus, the option **Allow Password Override (no key)** is only available to XyLoc users other than the designated administrator.

Configuring the XyLoc Software

Security Configuration and User Preferences

XyLoc's operating parameters are set through the **XyLoc Configuration Manager**. To launch the **XyLoc Configuration Manager**, select **XyLoc Configuration** from the **Start** menu (**Start/Programs/XyLoc/XyLoc Configuration**). You may also double click on the **ET** (XyLoc icon) in the **System Tray**.



The **XyLoc Configuration Manager** has two tabs from which XyLoc's operating parameters are set:

- User Setup
- PC Setup

NOTE: The XyLoc system is *NOT disabled* when the XyLoc Configuration Manager is running. If the system locks while the configuration manager is open, any unsaved changes will be lost.

NOTE: Starting with XyLoc version 8.3.5, if an XSS address is configured in the client, the settings in the configuration manager under "User Setup" will be entirely grayed out. All user settings must be managed from the XSS at that point. The settings in the "PC Setup" tab are still available.

User Setup

The screenshot shows the 'User Setup' dialog box in the XyLoc Configuration Manager. It is divided into two tabs: 'User Setup' and 'PC Setup'. The 'User Setup' tab is active and contains the following sections:

- User Settings:** Includes a 'Login Authentication' section with a 'Select User Name' dropdown menu and a checked 'Allow Password Override (No Key)' checkbox. Below it is an 'Unlock Authentication' section with another 'Select User Name' dropdown and a checked 'Allow Password Override (No Key)' checkbox. To the right is a 'User Name' list with 'Administrator' and 'Guest' options.
- Key Settings:** Includes a 'Range' dropdown set to 'Medium', a 'Range Refinement' button, and a 'Personal Name' text field containing 'Administrator'. Below this is a 'Key ID' field showing '0000012345'.
- Buttons:** 'Add User...', 'Delete User...', 'Add Key...', 'Delete Key...', 'Save', and 'Advanced Settings...'.

Callouts provide instructions for various elements:

- Login Authentication:** Select a log-on account from the **User Name** list to modify that user's settings.
- Allow Password Override (No Key):** Select **Allow Password Override (No Key)** to enable override access to the desktop from a locked state.
- Add User...:** Click **Add User...** to use the **Configuration Wizard** to add a new log-on account.
- Delete User...:** Click **Delete User...** to delete the selected account.
- Unlock Authentication:** Select the time during which the XyLoc will unlock the PC's desktop without requiring the user to enter a password.
- Range:** Shows the key or keys assigned to the selected log-on account.
- Add Key...:** Click **Add Key...** to use the **Key Wizard** to add a new key.
- Delete Key...:** Click **Delete Key...** to delete the selected key.
- Advanced Settings...:** Click **Advanced Settings...** to access additional settings.
- Range Refinement:** Click **Range Refinement** to make fine adjustments to the range at which desktop will lock/unlock.
- Personal Name:** Enter the **Personal Name** to associate a friendly user name with the selected account.

NOTE: A user's **Key ID** must be selected before the following options are available.

User Name

What It Does:

Shows the currently selected login account from the **User Name** list.

Recommended Use:

See **Adding New Users**.

Add User...

What It Does:

Enables you to add a network account for XyLoc to login with.

Recommended Use:

(See **Adding New Users**) This does NOT create a local Windows account on the machine. Local accounts must be created through Windows and will automatically show up in the XyLoc User Name window.

Delete User...

What It Does:

Enables you to delete a network account or remove all keys from a local account.

Recommended Use:

Does NOT remove local Windows accounts; this must be done through Windows if a user account is to be removed. Also see **Disable this Account**.

Key ID

What It Does:

Shows the unique number of the Key or Keys issued to a particular login account.

Recommended Use:

See **Adding New Keys** and **Kiosk Accounts**.

Add Key...

What It Does:

Enables you to add a new key for the selected user or kiosk account.

Recommended Use:

See **Adding New Keys** and **Kiosk Accounts**.

Delete Key...

What It Does:

Enables you to delete a key from the selected user or kiosk account.

Recommended Use:

Delete a key when the user has lost a key or when you want to remove a key from a kiosk account (see **Kiosk Accounts**).

Login Authentication

Hands-Free AutoLogon

What It Does:

User is automatically logged in without requiring that any other action be taken.

Recommended Use:

For maximum convenience and completely hands-free operation; if users are within set proximity of their PC, they will logged in.

Select Username

What It Does:
Finds all the keys in the area and then prompts the user to select their name.

Recommended Use:
This setting is useful for environments where many users are in a small area such as cubicles, labs, or the nurses' station at a hospital.

Must Enter Password

What It Does:
User must enter a password to login. The system finds the strongest key in the area and then prompts the user for a password.

Recommended Use:
For use in environments with a need for greater security. Administrators should also see **Allow Password Override** for information on settings for maximum security.

Allow Password Override (No Key)

What It Does:
Allows the user to login to the PC without requiring an authorized key.

Recommended Use:
Administrators should enable this setting if they want to allow user access without the XyLoc Key (e.g., when the user forgets his Key). If this option is unchecked the account cannot be accessed without a key. This provides maximum security, especially when used in combination with **the Must Enter Password** and **Select User and Enter Password** modes. XyLoc requires that at least one administrative account allow for password override as a safety precaution.
NOTE: By default a non-XyLoc user is able to use CTRL+ALT+DEL at a login screen and login to their account. This is to provide access for administrators. If you do not want to allow any non-XyLoc users to override, then there is a registry setting that can be enabled. Contact Ensure Technologies Technical Support for more details.

Unlock Authentication

Hands-Free Unlock

What It Does:

When an authorized user enters the **Active Zone**, the PC's desktop is automatically unlocked without requiring that any other action be taken.

Recommended Use:

This is the default setting and provides the most convenience.

Select User Name

What It Does:

Finds all the keys in the area and then prompts the user to select his key.

Recommended Use:

This setting is useful for environments where many users are in a small area such as cubicles, labs, or a nurses' station at a hospital.

Must Enter Password

What It Does:

User must enter a password to unlock the PC.

Recommended Use:

For use in environments with a need for greater security. Administrators should also see **Allow Password Override** for information on settings for maximum security.

Allow Password Override (No Key)

What It Does:

Allows the user to unlock the PC without requiring an authorized key.

Recommended Use:

Administrators should enable this setting if they want to allow the user to unlock without the XyLoc Key (e.g., when the user forgets his Key). If this option is unchecked the account cannot be unlocked without a key. This provides maximum security, especially when used in combination with the **Must Enter Password** and **Select User and Enter Password** modes.

Unlock to Key Only for up to x seconds/minutes

What It Does:

Enables a grace period in which PC will unlock to user by presence of authorized key alone.

Recommended Use:

For increased convenience in organizations, use this setting in situations where the system locks while the user is still in control of the PC (e.g., when the user turns away from the PC to get something out of a filing cabinet on the other side of her cube or office), and then returns to work at the PC within the specified time. After specified time, user must provide selected unlock authentication (e.g., a password).

Range

What It Does:

Defines the **Active Zone** by setting the range at which XyLoc will lock/unlock the PC.

Note: The numbers that are referenced for unlock and lock are not a reference to feet or meters. The numbers are a reference to strength of the signal between lock and key.

Recommended Use:

Choose **Short, Medium** or **Long** distance for XyLoc operation based on user preference and office size/environment.

Range Refinement

What It Does:

Permits fine adjustment of the Active Zone by opening the **Range Setting** box.

Recommended Use:

Select when minor adjustments of the Active Zone are desired.

Personal Name

What It Does:

Specifies the user's full name.

Recommended Use:

Enter the user's full name if you prefer additional user information beyond the user's login name. This is especially helpful in Audit logs and in Kiosk accounts.

Advanced Settings

What It Does:

Opens the **Advanced User Settings** window.

Recommended Use:

Click the **Advanced Settings...** button to modify **Administrative Level** and other settings.

Advanced User Settings

Allows this user account to logoff another user account that is in a locked state

Allows the **Key ID** to be changed to a new ID while maintaining existing settings

This timer delays the locking of a workstation when a key goes out of the defined lock range.

It is used by the **Kiosk Account** feature to provide multiple factor authentication in a shared log-on account

Used to lock the workstation automatically due to inactivity when in Password Override mode.

Select the **Administrative Level** for the selected user and key

Select the **Auto Logoff Time** to close an account after a period of inactivity after screen is locked

Select **Disable Key** to disable specific key from log-on account

Select to enable the **Pass Key** option for Administrators

Select to play the "Default" system sound when XyLoc secures the PC

Select to assist with preventing users from leaving key unattended

Used to run a configured Application Integration logoff script automatically when the PC is locked.

Administrative Level

Administrator

What It Does:

Gives full access to configure settings for all administrators, users and guests.

Recommended Use:

Given to the person or persons given the responsibility of managing an organization's computer security.

User

What It Does:

Gives access to configure the user's **Range Settings** and **Personal Name**; only the specific user's name is visible in the **User Name** field.

Recommended Use:

Given to a person who is authorized to make limited changes to the configuration settings.

Guest

What It Does:

Allows a person to use a PC without the ability to view or change any configuration settings

Recommended Use:

The most limiting level; no access to **XyLoc Configuration Manager**

Auto Logoff Time

What It Does:

After the authorized user leaves the active zone and the desktop locks, XyLoc starts an inactivity timer. If the logged-in user does not return before this time expires, the account is logged off. *For fastest multi-user access, also see Kiosk accounts.*

Note: Any data that was not saved by the user may be lost.

Recommended Use:

This is a secondary and less sophisticated method to provide automated log-off access to users. In general Ensure recommends the use of the **User can logoff locked workstation** feature as the primary method of logging-off users.

Auto Logoff allows you to prevent a locked PC from staying logged-on indefinitely. This feature can work independently or in conjunction with the **User can logoff locked workstation** function.

Note: This timer is in minutes only (whole numbers). The minimum time is one (1) minute after a lock event.

User can logoff locked workstation

What It Does:

Allows the user to log-off another user who logged on to and locked a workstation. *For fastest multi-user access, also see Kiosk accounts.*

Note: Any data that was not saved by the user may be lost

Recommended Use:

This is the primary and recommended method for logging-off users who lock a PC and then leave. When this option is selected, the XyLoc user will be able to force a log-off of another user's locked desktop.

With this option, the user forcing the logoff will need to select their name from the list. Once the logoff has occurred, the user will then use their normal login authentication.

Key ID

What It Does:

Lets administrators change the Key ID for this account.

Recommended Use:

This is useful when you desire to change an account's Key ID but maintain all existing settings. This allows the administrator to easily replace a lost or stolen XyLoc key.

Lock Delay

What It Does:

Delays the locking of a workstation for the defined time once a key is taken outside of the defined lock range.

NOTE: This feature does not delay the locking for other lock events such as turning the key off manually, locking the workstation manually, or locks due to the other different timers (i.e. Stationary Key and Password Override)

Recommended Use:

Would help reduce the number of undesired locks due to momentary interference (whether from the users own body or other “external” factors) with the RF signal from the key.

It would also be used in cases where a user needs to be away from the workstation at a distance that would normally lock the computer, but still needs to be able to view the screen for a period of time.

NOTE: The setting here is used on correlation with another setting in the PC Setup section of the Configuration Manager. The client will always use the larger of the two values (User vs. PC).

Pass Key

What It Does:

Lets administrators access the current user’s desktop without logging that person out.

Recommended Use:

This is useful in situations where the administrator needs to troubleshoot a problem that may be specific to a particular user’s account.

To use a XyLoc Key as a **Pass Key**, the **Pass Key** holder must approach the secured computer and press **Ctrl-Alt-Del** (under Windows 2000/XP). The **Pass Key** holder will then have to enter their user name and **XyLoc password** into the dialog box to gain access to the current user’s desktop. When the **Pass Key** user leaves the active range, the computer will relock.

NOTE: If the **Pass Key** user is also an Administrator under Windows 2000 and XP, the XyLoc Password **MUST** be different from the Windows password.

Beep When Locking

What It Does:

Plays the “Default “ system sound when XyLoc secures the PC.

Recommended Use:

Enable this setting initially to provide users with audio feedback when their PCs are secured. After users are familiar with XyLoc’s operation, they may no longer need or desire this feature.

Lock if the Key is Stationary for

What It Does:

Secures the computer's desktop automatically if the user leaves their XyLoc key next to their computer for the set time period.

Note: Ensure recommends the 1-minute option for demonstration purposes only.

Recommended Use:

Use to assist with enforcing compliance with security policy and to encourage the user to keep the XyLoc key with them at all times. The system senses that the strength of signal from the key is not varying enough, and secures the desktop after the specified time. A message noting a stationary key for this user is recorded into the Audit Log and sent to the XyLoc Security Server (XSS). **NOTE:** If other factors in the environment cause the signal from the key to vary, it is possible the signal could vary enough to keep from locking, even when stationary.

XyLoc Password

What It Does:

Sets the XyLoc password.

Note: This box will only appear if this key is part of a Kiosk Account.

Recommended Use:

It is used by the **Kiosk Account** feature to provide multiple factor authentication in a shared log-on account.

Lock in Password Override

What It Does:

Locks the PC after a period of inactivity in password override mode.

Recommended Use:

Enable this for when the users key has been forgotten and you wish the PC to lock after a period of inactivity. This is NOT the recommended use of XyLoc, as it does not take advantage of XyLoc's full-time proximity based security capabilities.

Run Application Integration Logoff

What It Does:

Executes a logoff script after the desktop has been locked for the specified amount of time.

Recommended Use:

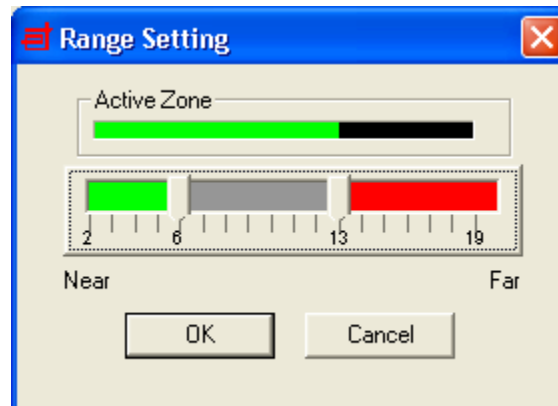
Works in conjunction with Application Integration. Recommended for use when a logoff script needs to be run so as to terminate an application or session.

Setting the Active Zone

Set the **Active Zone** by selecting the appropriate **Range** for your environment.



You can further refine this range with **Range Refinement**.



The top bar labeled “**Active Zone**” shows the approximate range where the computer will remain unlocked. Below this is an adjustable range scale. This permits the setting of “**Initial Unlock**” and the “**Lock.**” The **Initial Unlock** setting (shown in Green) sets the

approximate distance where the XyLoc will unlock the computer when the user returns. The **Lock** setting (shown in Red) is the approximate location where the computer will secure as the user steps away.

NOTE:

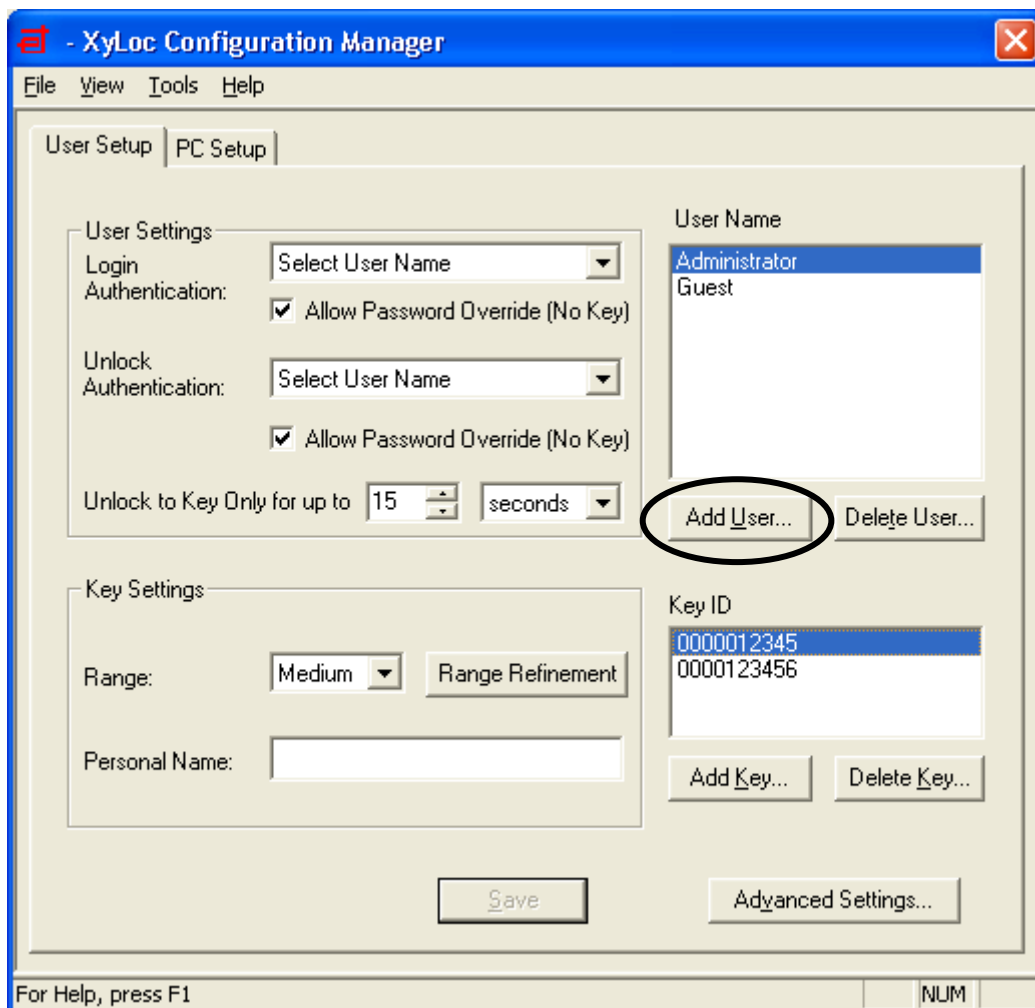
Given the nature of RF communications and the differing environmental characteristics of each user's office or cubicle environment, the precise **Active Zone** setting will vary for each user's environment. Ensure recommends that users initially selecting **Short** and then decide if **Medium** or **Long** is a more appropriate setting.

Further adjustments can be made within these three settings through the **Range Refinement** setting.

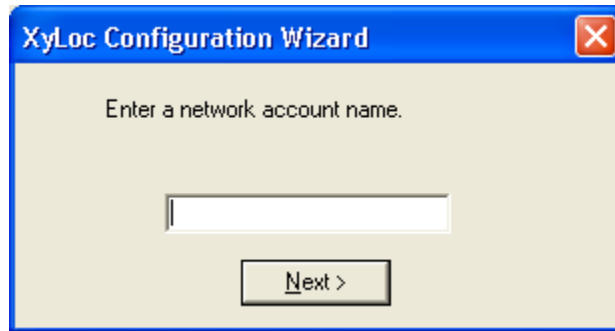
Adding New Users

The first user is created during **Installation** (see **Getting Started – Installing the XyLoc software**). All local accounts on a machine will appear in the **User Name** window of the **Configuration Manager** for an administrator to create XyLoc accounts from. You can also add existing network accounts to **XyLoc** by using the **XyLoc Configuration Manager’s Add User** button. **NOTE:** This will only add existing Microsoft or Novell network accounts to XyLoc. This does not actually create a new network account. The Network Administrator on the Microsoft or Novell server must do that.

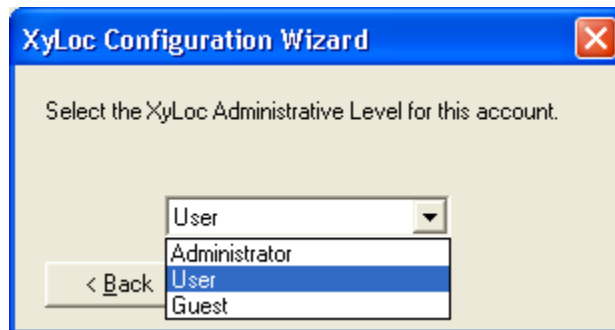
1. Click on the **Add User** button.



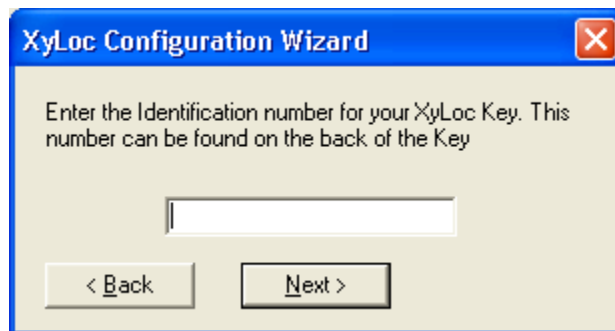
2. To create a new network user, enter a valid **user name** in the field and then click **Next** to proceed.



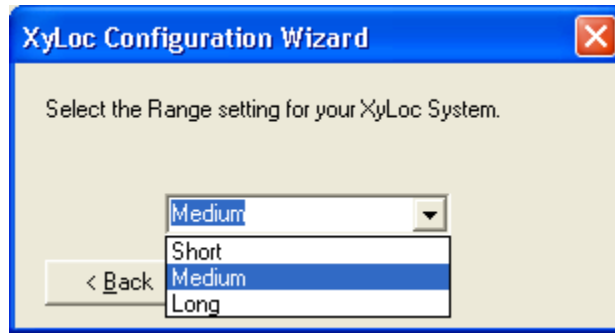
3. Select the Administrative Level for the new user. Click Next to proceed.



4. Enter the identification number for the **XyLoc Key** assigned to the new user.



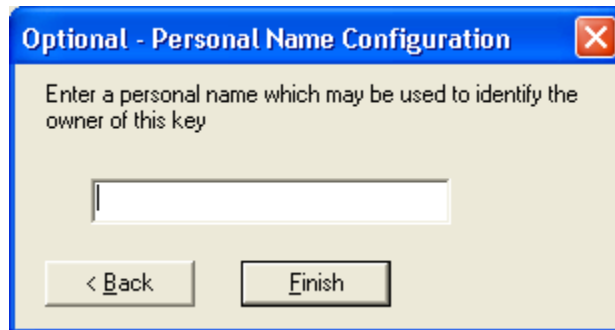
5. Select the **Range** setting for this Key



6. Select the **Authentication Methods** for this Key.



7. Finally, enter a personal name to be used to more identify the owner of this Key.

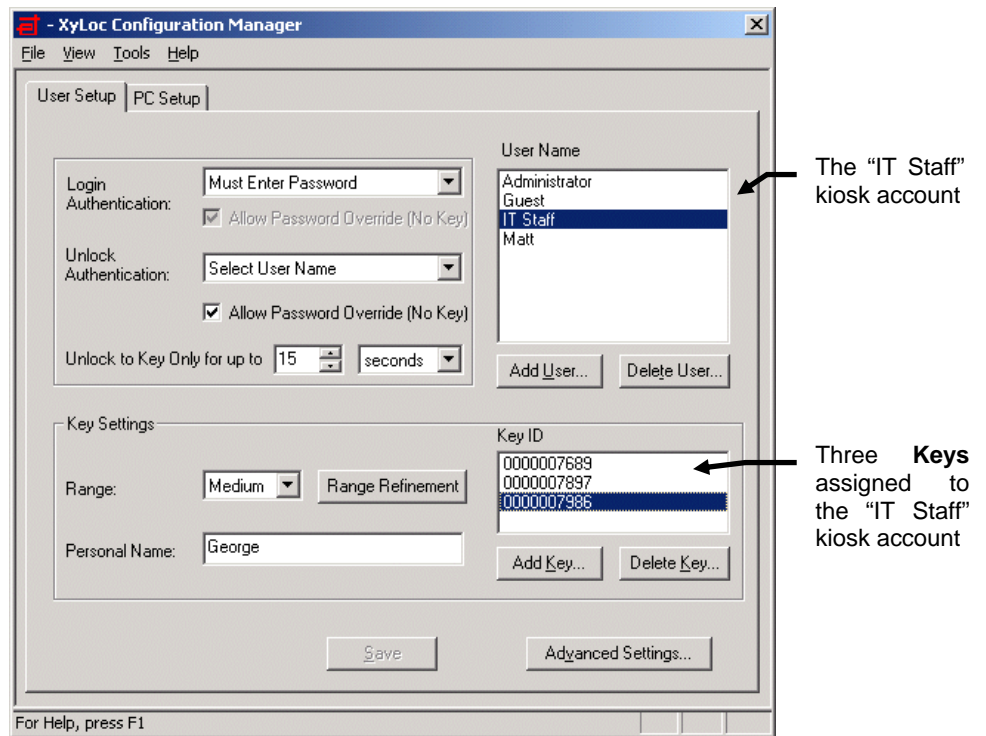


Kiosk Accounts

Workstation and network logins and logouts are often times several minutes in duration. In a multi-user environment, this delay can be frustrating. Ensure Technologies has developed a secure multi-user shared account feature that provides both security and fast multi-user access. In many settings, you may want to set up a single system account (Microsoft or Novell) for an entire class of users (for example, a “Nurses” account in a hospital or a “Sixth Grade Math” account in a school). You may easily set up such a “kiosk” account by adding multiple keys to the same account. In this Kiosk account, all users share the same XyLoc preferences except for **Range** and **XyLoc Password**.

This enables the shared use of a single account, while still tracking individual users’ access of the account in the XyLoc activity logs. Switching among users is fast and convenient.

NOTE: Support for Kiosk accounts in the XyLoc Solo package is limited to 5 users. The XSS-MD package is required for further support of Kiosk accounts. Please review the XSS User Guide for more detail on creating Kiosk accounts in that package.



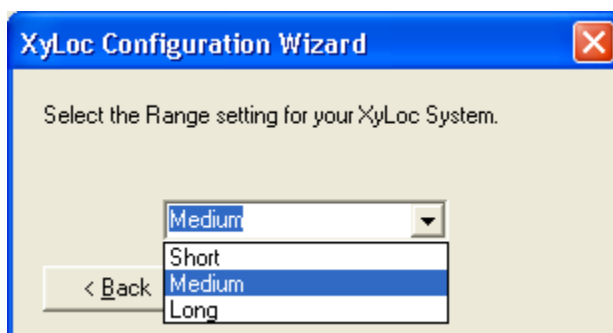
A kiosk account called “IT Staff” with three keys assigned to it.

Adding New Keys

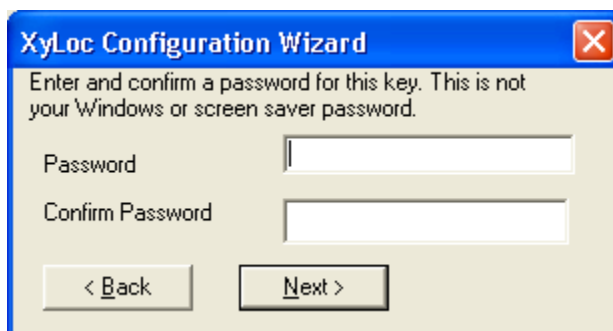
1. To create or add users to a **Kiosk Account**, simply select the user name in the **User Name** list and then press the **Add Key...** button. This will launch the **Key Wizard**. Enter the new Key number (found on the label on the back of the Key) and click **Next** to proceed.



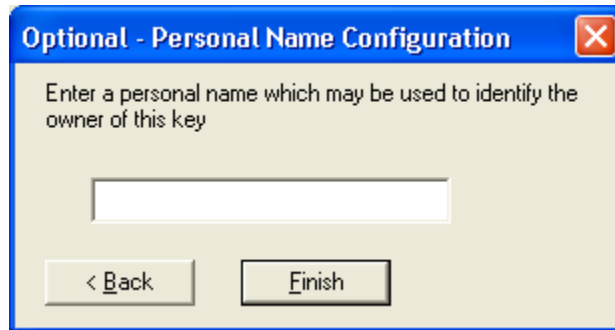
2. Select the **Range** for the new Key and click **Next** to continue.



3. Enter and confirm a unique **Password** for the new Key and click **Next** to continue (**NOTE**: This password is the “XyLoc Password” or “XyLoc PIN” that has been referenced in this document already. Starting in version 8.2.4, this password is the only password that is accepted when used in conjunction with the XyLoc Key. Previously, the client would also accept the Kiosk accounts own Microsoft/Novell password for login/unlock).

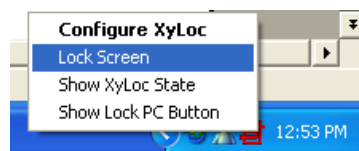


4. Finally, enter a personal name to be used to more fully identify the owner of this Key.



Locking the Desktop Manually

It is possible to manually lock the desktop. Right-click on the XyLoc icon and select **Lock Screen**.



This is useful when a user forgets his/her key and wants to manually secure the desktop before stepping away from the PC.

It is also possible to have a button available on the desktop to manually lock the desktop without having to right-click the icon. By default, this button is disabled. To activate this feature, right-click on the XyLoc icon and on the popup menu click on “Show Lock PC Button”. This will put a lock button right above the system tray on the desktop. The user can click this button at any time to manually lock the computer.



NOTE: Locking the desktop manually will require the user to re-authenticate to the PC before access is granted. If the user has a Key and manually locks the screen, the “Unlock to Key only” timer will not apply.

PC Setup

Select the port to which XyLoc is attached

Specify the number of log records to be uploaded to the XSS

Works with Application Integration. Sets one of the function keys to be used to launch a "Hot Trigger" Script.

Setting for use with the XyLoc Security Server. Enter the DNS name or IP address of the XSS server.

Click **Save** to keep any settings changes you have made

Click **Advanced Settings...** to access additional settings such as Logging Level

XyLoc Lock Attached To

What It Does:

Allows user to select and change the port to which XyLoc is attached.

Recommended Use:

This will be one of the available COM ports or the USB port. **NOTE:** Port selection will depend on the model of XyLoc Lock you are using.

XyLoc Security Server

What It Does:

Allows XyLoc installation to be centrally managed through a XyLoc Security Server (XSS).

Recommended Use:

Not used with XyLoc Solo installations. Please refer to 'User Guide for XSS-SQL' or 'XSS-AD' for additional details.

Log Records To Upload

What It Does:

Specifies the number of log records to upload to the XSS at a time.

Recommended Use:

Provides an Administrator the ability to manage traffic on the network between the XyLoc client and the XSS

Advanced Settings

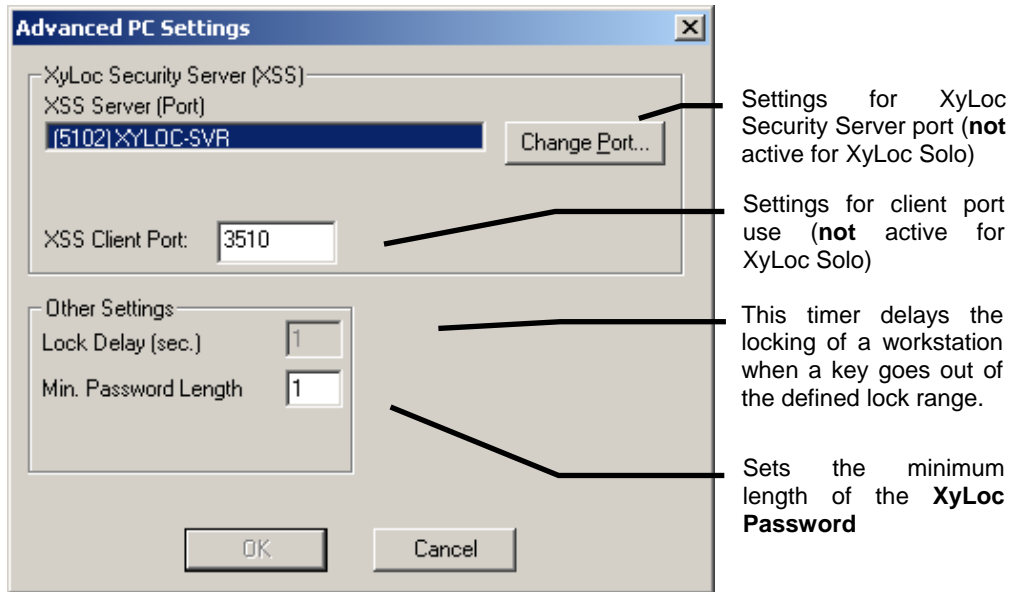
What It Does:

Opens the **Advanced PC Settings** window.

Recommended Use:

Click the **Advanced Settings...** button to modify **XSS** and **Password** settings.

Advanced PC Settings



Settings for XyLoc Security Server port (**not** active for XyLoc Solo)

Settings for client port use (**not** active for XyLoc Solo)

This timer delays the locking of a workstation when a key goes out of the defined lock range.

Sets the minimum length of the **XyLoc Password**

XSS Client Port

What It Does:

Allows XyLoc installation to be centrally managed through a XyLoc Security Server (XSS).

Recommended Use:

Not used with XyLoc Solo installations, but offers easy expansion and management of larger XyLoc installations. Please refer to XSS User Guide for additional details.

Lock Delay

What It Does:

Delays the locking of a workstation for the defined time once a key is taken outside of the defined lock range.

NOTE: This feature does not delay the locking for other lock events such as turning the key off manually, locking the workstation manually, or locks due to the other different timers (i.e. Stationary Key and Password Override)

Recommended Use:

Would help reduce the number of undesired locks due to momentary interference (whether from the users own body or other “external” factors) with the RF signal from the key.

It would also be used in cases where a user needs to be away from the workstation at a distance that would normally lock the computer, but still needs to be able to view the screen for a period of time.

NOTE: The setting here is used on correlation with another setting in the User Setup section of the Configuration Manager. The client will always use the larger of the two values (User vs. PC).

Min. Password Length

What It Does:

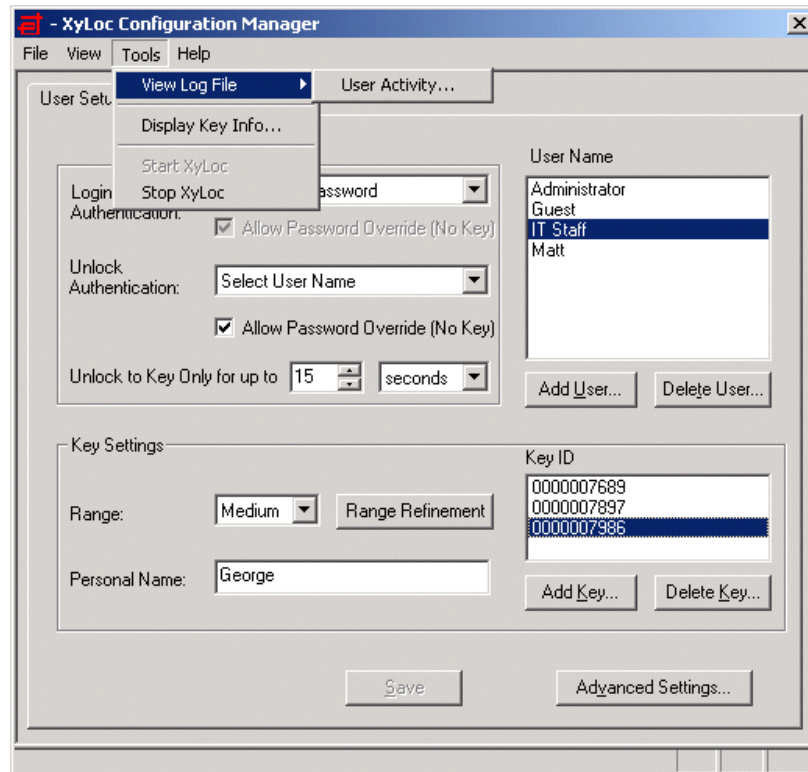
Determines the minimum acceptable password length for the **XyLoc Password**.

Recommended Use:

This should be set to at least **4** to provide robust security.

Logging

XyLoc will collect data to track **User Activity**. This encrypted log may be accessed under the **Tools** menu of the **XyLoc Configuration Manager**.



User Activity Log

What It Does:

Displays a history of each user that has logged on and logged off of the machine

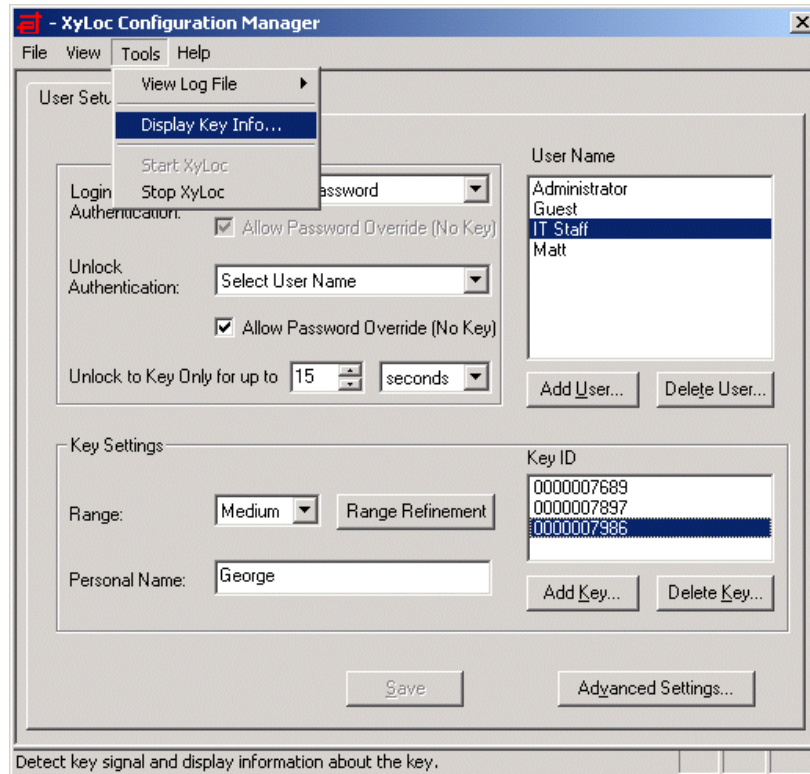
Recommended Use:

Track user activity, including dates and times.

NOTE: This option will only be available to a XyLoc Administrator.

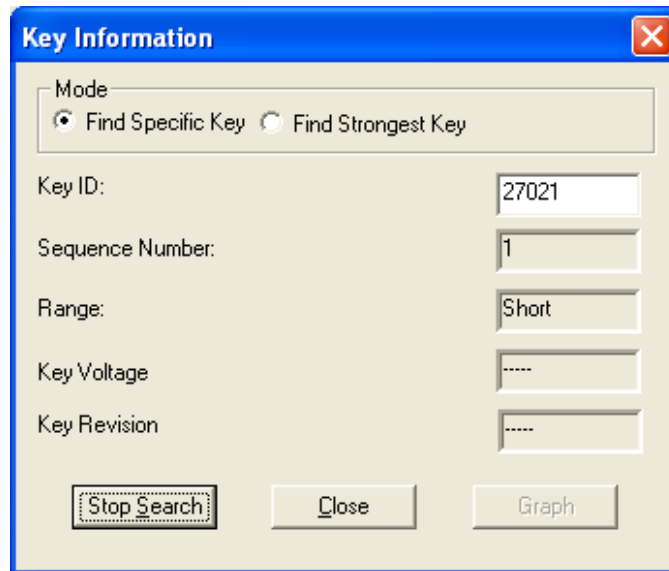
Testing XyLoc Keys

Selecting **Display Key Info...** from the **Tools** menu provides administrators with a diagnostic tool for identifying and testing XyLoc Keys.



The **Key Information** tool offers two modes: **Find Specific Key** and **Find Strongest Key**.

NOTE: The **Key ID** is located on the label on the back of the XyLoc Key



Find Specific Key Mode

What It Does:

Allows you to test a specified XyLoc Key

Recommended Use:

Select **Specific Key** mode and enter the **Key ID** in the Key ID field; click **Start Search** to test the Key.

NOTE: Only a XyLoc Administrator can view other keys and therefore change this setting from the active key.

Find Strongest Key Mode

What It Does:

Allows you to test the XyLoc Key with the strongest signal within 50 feet of the XyLoc Lock

Recommended Use:

Select **Find Strongest Key** mode and click **Start Search** to identify the XyLoc Key with the strongest signal; you can also use this function to determine or verify a **Key ID** by placing the XyLoc Key next to the XyLoc Lock.

NOTE: Only a XyLoc Administrator has this setting available.

Sequence number

What It Does:

Displays the ID of the last data received from the Key; the number should update every 1-2 seconds

Recommended Use:

Lets you know that Key and Lock are communicating properly

Range

What It Does:

Displays the current range of the Key from the Lock

Recommended Use:

Use this value to help determine the optimal **Range** for your environment

Key Voltage

What It Does:

Displays the current voltage of keys that support this function.

Recommended Use:

While the system is searching for the key, press the “O” button on the key and the voltage will be displayed.

Key Revision

What It Does:

Displays the current revision of the key.

Recommended Use:

Use to determine the revision of the key when instructed by Ensure Technologies Technical Support.

Overriding the XyLoc System

There will be times when it is necessary to override the XyLoc system. At login, there are two basic methods of overriding the XyLoc system. One is for a XyLoc user that has a badge that is authorized on the PC, but has forgotten it or lost it. The other is for a user that does not have a XyLoc badge assigned, yet still needs to gain access to the PC.

User Forgets Their Key...

In the event a user forgets or loses the Key, pushing the Password Override button on either the Login or Locked Workstation screens and entering the user's Login and Password will override the system. The user can enter either their standard Microsoft username/password, or they can enter their XyLoc Personal Name in conjunction with their XyLoc Password (in a Kiosk account). Using the personal name enables XyLoc to correctly identify the specific user in a Kiosk account when many users are sharing a single username.

However, if the **Allow Password Override (No Key)** option is unchecked, the user will not be able to access their account if the key is not present. The XyLoc system software ensures that there is always at least one administrator that can password override into a machine.

NOTE: Make sure that your XyLoc installation is working with **the Allow Password Override (No Key)** checked before un-checking the option. You will not be able to gain access to your computer if the Key is missing (or not functioning properly) or if you forget your password.

Once access is obtained with this password, XyLoc is overridden and in a standby mode. The XyLoc icon in the System Tray will have a slash through it, indicating that the XyLoc system is no longer actively protecting your system:



XyLoc will resume protecting your PC when one of the following occurs:

1. The user manually locks the PC.
2. The user manually restarts the PC or logs off from the current session.
3. If system is idle for longer than the time specified in the **Lock in Password Override**.
4. The authorized XyLoc Key is returned to the active range (XyLoc will recognize the presence of the authorized Key and the status will change accordingly. **NOTE:** If the user is in a Kiosk account, they must perform the override using the Personal Name/XyLoc Password combination in order for XyLoc to recognize the proper Key for the user. If the standard Microsoft credentials are used for override, XyLoc will ignore all keys assigned to that account for security reasons.

User Does Not Have a XyLoc Key...

If a user does not have a XyLoc key assigned to them, or has a XyLoc key but this key has not been configured as an authorized key on a particular PC, the user can still gain access to the PC using the standard Ctrl+Alt+Del keystroke combination. This user will be bypassing the XyLoc security and will login with their account. They will have whatever permissions assigned to them network or PC. Administrators or Helpdesk staff mostly use this to allow them access to a PC when they don't have a XyLoc key. There is a registry setting available to disable any non-XyLoc user from gaining access to a XyLoc protected PC, however this is not recommended unless the centralized server (XSS) is available as this does restrict ALL non-XyLoc users including Administrator. Contact Ensure Technologies Technical Support for more details.

Unlocking using Password Override...

At unlock, either process can be used to get a dialog box to enter credentials in and either method can be used. However, the user must use the same as was used at the initial login. Once an account is logged into the PC, only that same account can unlock the PC using Password Override.

Using Microsoft Remote Desktop Protocol (RDP)

Beginning XyLoc Client version 8.5.6, significant improvements were corrected in the RDP functionality included in the Microsoft operating system of a XyLoc workstation.

Authorized Microsoft "Remote Users" of the XyLoc workstation can connect with the XyLoc client installed on the workstation.

For a complete overview of using RDP with the XyLoc Client, please refer to the document number 530-0200-020, "*Using RDP with XyLoc Client*"

Replacing the XyLoc Battery

The KeyCard is powered by a single coin cell (CR3032) that lasts approximately 8-12 months. A user may check the battery by depressing the switch marked “O” on the key. If the battery is good, a Green LED will momentarily flash. The user is able to check the battery life through the XyLoc configuration software.

Replacement batteries may be purchased at a local electronics distributor, directly through Ensure Technologies or your local reseller. You can also find these batteries at <http://digkey.com/>. Their part number is P121-ND.

To replace the XyLoc battery:

1. Flip over the Key
2. You will see the battery compartment with the tab
3. Remove the two retaining screws from the battery compartment
4. Slide open the top of the battery compartment
5. Remove the battery and replace it with the new battery, observing proper polarity indicators (+ side up)
6. Slide compartment cover to close and replace the screws

Software Removal

In the event that you have to remove the XyLoc client software, please use the following instructions:

1. Before you can remove the software, you must stop the XyLoc service. This can be done through the Services applet in the Control Panel in Windows, or through the XyLoc Configuration Manager under Tools -> Stop XyLoc (NOTE: You must be a system administrator to stop a Windows service, and if done through the configuration manager, you must also be a XyLoc Administrator.
2. Once the services are stopped, you can close the XyLoc Configuration Manager (if open) and then go to the Windows Control Panel and then to “Add/Remove Programs”. From here select the “XyLoc Security Service” and remove it.
3. After removal, you will need to reboot.
4. Once the system is rebooted, you can delete the Ensure Technologies directory under Program Files.
5. The USB drivers do NOT get removed during this process. This way if you wanted to reinstall, you don’t have to go through the device installation again. However, if you want to remove the device, follow the standard process for uninstalling a device in Windows.

Troubleshooting

Please refer to the solutions to common setup problems below. If you still cannot resolve the problem, please call Ensure Technologies Technical Support at (734) 547-1600, or send an email to support@ensuretech.com.

Helpful Hints:

1. Use the default settings until you become familiar with XyLoc's operation.
2. The XyLoc application requires that at least one network protocol be loaded on the PC to properly load and operate. For example, most PC's commonly have protocols such as TCP/IP or NetBEUI loaded by default. Either or both of these meet the requirement.
3. **Windows 2000/XP:** An administrator or a user with FULL, local administrator privileges is required to install the XyLoc system.
4. **Windows XP Fast-User Switching:** Microsoft's Fast-User Switching feature is not designed to operate in a network environment (reference Microsoft TechNet article Q294739). Ensure Technologies supports Windows XP in a network environment. The XyLoc Kiosk account provides this type of functionality. Please contact Ensure Technologies for further information.
5. The XyLoc icon in the System Tray can be used to view the status of your system and to help troubleshoot the system. Simply move your cursor over the XyLoc icon to view the current status of the XyLoc system.
6. When running Scandisk or Disk Defragmenter and experiencing disk restarts, you should stop XyLoc. Once Scandisk or Disk Defragmenter has completed, re-start XyLoc.
7. The use of a screen saver may no longer be necessary or desired. In Windows 2000/XP, the Microsoft GINA controls the password protection. Since the XyLoc GINA has taken over control of the security of the PC, the password protection is automatically disabled. The screen saver functionality will still take place, however it will no longer be password protected. This is no longer necessary, since the PC will automatically lock when the user takes their Key out of range. Use the "Lock in Password Override" timer to provide the same protection when in Password Override mode.
8. If your monitor has been turned off as a result of using Power Management or Energy Saving mode, or if a screen saver has activated, a key press or mouse movement may be required to activate your PC even though the authorized XyLoc Key has already unlocked the computer.
9. **Windows Power Management:** At this time, Suspend/Hibernate in Windows 2000/XP are not fully supported. Ensure Technologies recommend that these features not be used.
10. **Windows XP Embedded Thin Clients:** The XyLoc client, when installed on XPe, does not support languages other than English at this time. Earlier versions did erroneously allow the user to select other languages. However, English is the only option that will install successfully.

System Functionality

Normal Operational Mode

The majority of users will use XyLoc in “Normal Operational Mode.” In normal operation, the XyLoc Lock and Key are in constant, encoded wireless communication with each other, with the Lock searching for the presence or absence of authorized Keys. As an authorized user approaches the PC, XyLoc responds and the Key and the Lock engage in an over-the-air authorization. Once XyLoc identifies and authenticates the user, it unlocks the PC until the user moves out of the **Active Zone**.

When the authorized user moves out of the **Active Zone**, XyLoc automatically blanks the screen, locks the keyboard and disables the mouse. The PC is instantly secured and remains so until an authorized user moves back inside the **Active Zone**. Background tasks, such as printing and downloading, however, may continue while the PC is securely locked.

Hardware Architecture

Both the Lock and the Key incorporate two embedded controllers, which allow the operating firmware to be updated in the field so new features can be added.

The Lock can receive firmware updates via the USB port. This firmware is stored in flash memory and is used to control the operation of the system. The communications controller controls the Lock-to-host communications, and is permanently programmed. The Lock also incorporates an EEPROM that stores operational parameters, such as channel allocations.

The Key has a similar architecture and can receive firmware updates via a proprietary programming cable attached to a PC.

Radio Frequency (RF) System

XyLoc operates in the 900 MHz frequency band – the same radio frequencies used by cordless telephones and other common wireless devices. Its power output is lower than cordless phones and far less than that of the cellular phones many people use every day. XyLoc is as safe to operate as any common household communication device, such as a cordless phone or baby monitor.

The operating frequency is set at the factory and cannot be changed out of the certified band by the end user. The power output level is also set at the factory and cannot be changed by the end user.

The XyLoc RF link uses a combination of spatial spectral reuse and time-division multiple access (TDMA). This combination of techniques improves the integrity of the RF link and insures that other radio devices will not interfere with XyLoc’s proper operation.

Spectral Reuse

Like a cellular phone system, a large XyLoc installation can effectively reuse spectrum across a facility by intentionally limiting the range of individual XyLocs. This allows Keys in different parts of a building to operate using the same frequencies at exactly the same time.

Time Division Multiple Access (TDMA)

Keys that are within range of each other can also reuse the same channel allocation by the use of time-division multiple access. This allows several hundred Keys to coexist within a 50-foot radius. As the Keys move through the building, they adaptively find new time slots to avoid interference with other Keys in that area.

Technical Specifications

Detailed Technical Specifications are available by contacting Ensure Technologies Technical Support at support@ensuretech.com or by phone at (734) 547-1631.

Revision History

Revision	Date	Description	Author
1.00	07-25-2009	Created	TR
1.01	08-18-2009	Updated with additional Delay Lock details	RS